PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-202694

(43)Date of publication of application : 27.07.2001

---

(51)Int.Cl. G11B 20/10

G06F 12/14

G09C 1/00

G11B 20/12

G11B 27/00

H04L 9/08

---

(21)Application number : 2000-170599 (71)Applicant : MITSUBISHI

CHEMICALS CORP

(22)Date of filing : 07.06.2000 (72)Inventor : KANAYAMA MASAAKI

FUJIWARA TAKESHI

---

(30)Priority

Priority number : 11177470

11319514

Priority date : 23.06.1999

10.11.1999

Priority country : JP

JP

---

(54) RECORDING MEDIUM, INITIALIZATION METHOD OF THE MEDIUM, CIPHERING METHOD ON THE MEDIUM, CIPHERING DEVICE, DECIPHERING DEVICE AND ACOUSTIC/VIDEO/DATA DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To protect copyrighted data by conducting a prescribed initialization for a CD-R disk or a CD-RW disk employing an existing format method so that a user is able to copy copyrighted data such as music, movie and computer program data on a disk for only once and no secondary copying is conducted from the copied disk to other disk.

SOLUTION: A CD-R disk (or a CD-RW disk) 10 is produced as a specific disk 10' in which a media number 1 that is a ciphering key prepared y combining six figure decimal number disk ID, thirteen figure decimal number MCN and five figure decimal number ISRC serial number and ciphered data 14 which are ciphered by the number 1 are recorded.

LEGAL STATUS [Date of request for examination] 10.11.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] It is the record medium which is the field which a reader can read, and a user offers the management domain which cannot access the field, and the data area where it is the field which this reader can read, and a user can access

the field at arbitration, and is characterized by recording the disk identification information for encryption on this management domain.

[Claim 2] The record medium according to claim 1 characterized by distributing and recording the medium identification number information which a user can read on it while media information including voice, an image, and any one information on the data was recorded on this data area as encryption media information enciphered by the cryptographic key generated using this disk identification information at least.

[Claim 3] The record medium according to claim 1 or 2 with which this record medium is characterized by what is recorded on optical.

[Claim 4] It is a record medium given in any 1 term of claim 1 - claim 3 to which this data area is characterized by being written in once [at least] by the user.

[Claim 5] It is the initialization approach of a record medium characterized by being the field which a reader can read, and for a user being the initialization approach of a record medium of having offered the management domain which cannot access the field, and the data area where it is the field which this reader can read, and a user can access the field at arbitration, and recording the disk identification information for encryption on this management domain.

[Claim 6] The 1st write-in step which records the disk identification information for encryption on this management domain in recording this disk identification

information, The 2nd write-in step which records medium identification number information on this data area by the mode dimorphism formula of a Q channel sub-code, The initialization approach of a record medium according to claim 5 characterized by having offered the 3rd write-in step which records serial number information, and mode 3 formats of a Q channel sub-code being consisted of by this data area.

[Claim 7] The management domain where it is the field which a reader can read and a user cannot access the field, It is the field which this reader can read and is the encryption approach on the record medium with which the user offered the data area which can access the field at arbitration. After performing initialization which records the disk identification information for encryption on this management domain By enciphering by the cryptographic key using the above-mentioned disk identification information at least, and recording media information including voice, an image, and any one information on the data on this data area as encryption media information The encryption approach on a record medium characterized by having offered the encryption step which generates a specific record medium, and being constituted.

[Claim 8] The encryption approach on a record medium according to claim 7 characterized by consisting of a 1st write-in step at which this initialization records the disk identification information for encryption on this management

domain, a 2nd write-in step which records medium identification number information on this data area by the mode dimorphism formula of a Q channel sub-code, and a 3rd write-in step which records serial number information on this data area in mode 3 format of a Q channel sub-code.

[Claim 9] The 1st disk identification information read-out step from which this encryption step reads this disk identification information as the 1st disk identification information, The 1st cryptographic key generation step which generates this 1st cryptographic key combining this 1st disk identification information and at least one information in this medium identification number information and this serial number information, The 1st read-out step which reads this media information from an external device, and by generating this encryption media information using this 1st cryptographic key, and recording on this data area that has this 1st disk identification information The encryption approach on a record medium according to claim 7 or 8 characterized by having offered the specific record-medium generation step which generates this specific record medium, and being constituted.

[Claim 10] The management domain where it is the field which a reader can read and a user cannot access the field, The data area where it is the field which this reader can read, and a user can access the field at arbitration is offered. The read-out means which can read at least this disk identification information in the

record medium with which the disk identification information for encryption was recorded on this management domain, The encryption media information generation means which enciphers media information including voice, an image, and any one information on the data to this data area, and may be outputted to it as encryption media information by the cryptographic key using the above-mentioned disk identification information at least, Encryption equipment characterized by having offered an encryption media information preservation means by which this encryption media information could be saved in this data area of the record medium which has the same disk identification information, and being constituted.

[Claim 11] The management domain where it is the field which a reader can read and a user cannot access the field, While offering the data area where it is the field which this reader can read, and a user can access the field at arbitration and recording the disk identification information for encryption on this management domain The 2nd read-out means which can read at least this disk identification information in the record medium with which the information enciphered by this data area was recorded, A 2nd cryptographic key generation means to generate the 2nd cryptographic key from this disk identification information at least, Decryption equipment which decodes the enciphered this information using this 2nd cryptographic key, and is characterized by having

offered the decryption means which can reproduce media information including voice, an image, and any one information on the data, and being constituted.

[Claim 12] The management domain where it is the field which a reader can read and a user cannot access the field, The data area where it is the field which this reader can read, and a user can access the field at arbitration is offered. The read-out means which can read at least this disk identification information in the record medium with which the disk identification information for encryption was recorded on this management domain, The encryption media information generation means which enciphers media information including voice, an image, and any one information on the data, and may be outputted as encryption media information by the cryptographic key using this disk identification information at least, The sound, image, and data station characterized by having offered an encryption media information preservation means by which this encryption media information could be saved in this data area, and being constituted.

[Claim 13] The management domain where it is the field which a reader can read and a user cannot access the field, While offering the data area where it is the field which this reader can read, and a user can access the field at arbitration and recording the disk identification information for encryption on this management domain The 2nd read-out means which can read at least this disk identification information in the record medium with which the information

enciphered by this data area was recorded, A 2nd cryptographic key generation means to generate the 2nd cryptographic key from this disk identification information at least, The sound, image, and data station which decodes the enciphered this information using this 2nd cryptographic key, and is characterized by having offered the decryption means which can reproduce media information including voice, an image, and any one information on the data, and being constituted.

[Claim 14] A record medium given in any 1 term of claim 1 - claim 4 which are characterized by performing this encryption using the information which combined the serial number information or these which were recorded on the frame of mode 3 format of a Q channel sub-code by the medium identification number information list recorded on the frame of the mode dimorphism type of this disk identification information and a Q channel sub-code.

[Claim 15] A record medium given in any 1 term of claim 1 - claim 4 which be characterize by perform this encryption using the random number function which use as a seed information which combined the serial number information or these which be recorded on the frame of mode 3 format of a Q channel sub-code by the medium identification number information list recorded on the frame of the mode dimorphism type of this disk identification information and a Q channel sub-code .

[Claim 16] a record medium given in any 1 term of claim 1 - claim 4 which be characterize by perform this encryption using the Hash Function which use as a seed information which combined the serial number information or these which be recorded on the frame of mode 3 format of a Q channel sub-code by the medium identification number information list recorded on the frame of the mode dimorphism type of the key message in which bit length be change and it deal , this disk identification information , and a Q channel sub-code .

[Claim 17] The initialization approach of a record medium according to claim 6 characterized by performing this encryption using this disk identification information and the information which combined this serial number information or these with this medium identification number information list.

[Claim 18] The encryption approach on a record medium according to claim 8 or 9 characterized by performing this encryption using this disk identification information and the information which combined this serial number information or these with this medium identification number information list.

[Claim 19] The encryption approach on a record medium according to claim 8 or 9 characterized by performing this encryption using the random-number function which uses as a seed this disk identification information and information which combined this serial number information or these with this medium identification number information list.

[Claim 20] The encryption approach on a record medium according to claim 8 or 9 characterized by performing this encryption using the Hash Function which uses as a seed the key message in which bit length is changed and it deals, this disk identification information, and information which combined this serial number information or these with this medium identification number information list.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention is used for CD-R (CD-Recordable), CD-RW (CD-Rewritable), recordable DVD (Digital Versatile Disc), etc., and it is related with the initialization approach list of a suitable record medium and a suitable record medium at the encryption approach on a record medium, and an encryption equipment list, and it relates to a decryption equipment list in sound, an image, and a data station.

[0002]

[Description of the Prior Art] in recent years, the product development of CD-R

(CD-R media or a CD-R disk may be called hereafter) and CD-RW (CD-RW media or a CD-RW disk may be called hereafter) which can write data in optical should do -- read-only Music CD, read-only CD-ROM, etc. -- in addition, the CD market is activated.

[0003] These groups are called CD family and have classes, such as CDDA, CD-MIDI, CDV, CD-G, and CD-ROM. Here, CDDA is called the so-called music CD and is an object for record playback of a digital audio signal. Moreover, CD-MIDI, CDV, and CD-G are used for record playback of a personal computer. On the other hand, CD-ROM is a read-only memory and photo CD, a video CD, etc. adapting this are used.

[0004] On the other hand, CD-R and CD-RW can write on a user. By these appearances, creation of CD can be performed now also at office or a home. Here, CD-R is refreshable at the CD-ROM drive carried in the personal computer, and can record mass data. It can write in only the hemihedry and once, and elimination of the once recorded data cannot be performed, and neither the disk which wrote in accidentally and was carried out, nor the disk which became unnecessary can be reused.

[0005] On the other hand, unlike CD-R, rewriting of data is possible for CD-RW. Elimination of 1000 times or more of data is possible for this CD-RW, and it can perform temporary preservation of mass data and trial writing of data. The price

of the hemihedry and a disk is more expensive than CD-R, and the recorded disk can be played only by the correspondence drive of a CD-RW drive etc.

[0006] Moreover, in recently, read-only DVD (Digital Versatile Disc) and read-only DVD-ROM with one several times the capacity of CD are produced commercially, and development of the medium which the user corresponding to such a high density medium can write in is performed briskly. For example, media rewritten 1000 times or more, such as a medium which can be written in only at once [, such as DVD-R,], and DVD-RAM, DVD-RW, are being developed.

[0007] Next, the writing of the data and a procedure with a physical format are explained by making CD-R/RW into an example using drawing 26 from drawing 24 . In addition, under the following explanation and in a drawing, in case two, CD-R and CD-RW, are called collectively, it may be written as CD-R/RW. Drawing 24 is drawing showing arrangement with the non-data area of CD-R/RW, and a data area. The disk 60 shown in this drawing 24 comes to offer a management domain 61 and a user area 62.

[0008] the field where a user can do neither direct read-out nor writing as for this management domain 61 -- it is -- this management domain 61 -- PCA (Power Calibration Area) and PMA (Program Memory Area) from -- it becomes. Here, the control information for adjusting the strength of laser in case PCA writes in data is stored. And the strength of laser is optimized by the information recorded

on this PCA to compensate for fluctuation of external factors, such as coloring matter of a CD-R disk, and supply voltage, operating temperature, etc.

[0009] Moreover, disk ID for identifying each disk by CD-R / RW drive, in case it writes first in a part of PMA of a CD-R disk or a CD-RW disk (disk identification information: Disc Identification) It is recorded by 6 figures of decimal numbers, and 19.9 bits. Next, a user area 62 (refer to drawing 24) is a field where data with actual music data etc. are recorded.

[0010] And a user area 62 consists of lead-in groove field 62a, data area 62b, and lead-out field 62c further. Here, data area 62b is the record section of actual data. Information, such as a data start point at the time of writing data in this data area 62b and a halting point, is recorded on lead-in groove field 62a and lead-out field 62c, respectively. Moreover, the writing of data is performed for that (it is called a session) from which such lead-in groove field 62a and lead-out field 62c became a pair as one unit.

[0011] The method of the writing to this disk is [a Disk-at-Once (Disk At Once) method and] Track AT Once (Track At Once). There are a method and a packet-writing (PacketWrite) method. A Disk-at-Once method means the method with which data are written in at a stretch toward a periphery from the core of a disk, and first, data are written in and Track At Once system means after that the method with which the control information for 60 seconds (lead-in groove) and

the control information for 90 seconds or 30 seconds (lead-out) are added before and after the data. And although succeedingly recorded behind the data with which the method which a packet-writing method can advance Track At Once system further, and can repeat record by the short data unit was said, and data were written in last time in CD-R, it is discretely (at intervals) recordable on each [of a disk] location like [in CD-RW] a floppy (trademark) disk etc.

[0012] Since data cannot be written in the remaining part even if an availability is in CD-R / RW disk if it writes in by the Disk-at-Once method, when the availability remains in CD-R / RW disk, Track At Once system or a packet-writing method is preferably used so that the postscript of data can be performed. Moreover, the session ATTOWANSU (Session At Once) method which is a like and records a lead-in groove, data, and lead-out on Track At Once system at this order has also been recognized recently.

[0013] The above-mentioned lead-in groove field 62a is equivalent to the field of the beginning of each session on CD-R, and is not written in at all at first. Moreover, while the writing of a session is not completed, TOC is written in, after being put into the next write-in address on a disk and completing the writing of a session. This TOC (Table Of Contents) It is the information written in a user area 62, and the information on a track number, a start point, and a halting point is said. Moreover, the numbers of trucks currently recorded on CD, those starting

positions, etc. are recorded, and TOC is functioning as a table of contents of a session.

[0014] Furthermore, lead-out field 62c is a field in the last of a session, and is used for having arrived at the last of data being shown. In addition, no data are written in. Drawing 25 is drawing showing the disc data structure in the middle of write-in. The left-hand side of this drawing 25 is the core of a disk 60, PCA, PMA, and lead-in groove field 62a, data area (program field) 62b, and lead-out field 62c are arranged from the direction nearest to this core, and most right-hand side is a rim. The band which is shown in this drawing 25 and by which the network cliff was carried out means that data are written in, in the middle of write-in [of CD-R], data are written in PCA, PMA, and data area 62b, and the information on a track number, a start point, and a halting point is saved temporarily.

[0015] Although drawing 26 is drawing showing the disc data structure after write-in termination and nothing is written in PCA on a disk 60, and PMA, TOC is written in lead-in groove field 62a, music data etc. are written in data area 62b, and the termination location is further written in lead-out field 62c. Now, record of data is performed per block (sector) to the physical format mentioned above. Next, this logical format is explained using drawing 38 from drawing 27 .

[0016] Drawing 27 is drawing showing a format of a subcoding frame. The block

(sector) 53 shown in this drawing 27 consists of 98 frame 53a. And block 53 has the sub coding region 54 and data area 54a. Here, data area 54a is a field where data, such as music, are recorded.

[0017] Moreover, the sub coding region 54 is a field which records information, such as a movement number of a silent part and music, an index, time amount, and an alphabetic character, and is recorded on data area 62b (refer to drawing 24) with data, such as music. It is not used in this sub coding region 54 being independent (every break), but one information is expressed with 98 continuous frames.

[0018] Moreover, drawing 28 is drawing showing a detailed format of frame 53a, and frame 53a shown in this drawing 28 has each field of a frame alignment signal, subcoding, data, parity, data, and parity. And it has 1 byte of field for subcoding, and 24 bytes of field for data. And 98 of this frame 53a gather, 2352 (24x98) cutting tools' block 53 is constituted, and it functions as information fields, such as a movement number of a silent part and music, an index, time amount, and an alphabetic character.

[0019] Drawing 29 is drawing having shown this sub coding region in the detail. A synchronizing signal is stored in 2 bytes of first field, and, as for the sub coding region 54 shown in this drawing 29 , information is recorded on it by other fields. Specifically, these channels are as follows. That is, the silent part by which the P

channel is inserted between music is recorded. Elapsed time, absolute time, etc. are recorded. [in / in Q channels / the frame of the movement number of music, the index number in a movement, and music] Moreover, as for R, S, T, U, V, and W, the text for the display of karaoke etc. is recorded.

[0020] And one bundle of a frame 98 and the attached lengthwise direction constitutes one channel from a frame 3 like field 54b shown in this drawing 29 . That is, Q channels are formed by 96 bits of Q1 to Q96. Moreover, the same is said of each channel of P, R, S, T, U, V, and W. Next, the mode of Q channels is explained. These Q channels have the mode format that three kinds of formats from the mode 1 to the mode 3 differ. Although Q channels take the format in the mode 1, they are fixed frequency and usually take the format in the mode 2 and the mode 3.

[0021] Drawing 30 is drawing showing the frame structure in the mode 1 of Q channels. Information is transmitted by the frame 55 of mode 1 format shown in this drawing 30 . Drawing 36 is drawing showing the 1st example of data logging. As shown in this drawing 36 , a Q channel field is recorded in mode 1 format, and data are stored in a data area. Drawing 31 is drawing showing the frame structure in the mode 2 of Q channels. The frame 56 in the mode 2 shown in this drawing 31 is a different format from a frame 55, and the frequency where this frame 56 appears is 1 block in rate at least 100 of Q channels. And N1-N13 of

this drawing 31 are a field which consists of 4 bits, respectively, and are MCN (Media Catalog Number) to these fields N1-N13. It is recorded with 13 figures (43.2 bits) of decimal numbers. In this MCN, it is the identifier of a media number. Moreover, drawing 32 is drawing showing the data format at the time of drive equipment recording MCN, and if drive equipment records according to this data format, the frame structure shown in drawing 31 will be recorded on a disk in fact. Moreover, drawing 33 is drawing showing a format of the MCN data which drive equipment read, and shows the data format at the time of reproducing the frame structure.

[0022] Drawing 37 is drawing showing the 2nd example of data logging. As shown in this drawing 37 , it is recorded by the mode dimorphism formula between mode 1 formats of a Q channel field. Moreover, in the data of the mode dimorphism type in that case, it is MCN, 1234567890123 [for example,]. It is stored. Drawing 34 is drawing showing the frame structure in the mode 3 of Q channels. Q frequency where the frame 57 in the mode 3 shown in this drawing 34 appears is also 1 block inside at at least 100 blocks. And ISRC (International Standard Recoding Code) is recorded on I1-I12 of this frame 57, among these it is a serial number (Serial Number) to I8-I12. It is recorded with 5 figures (16.6 bits) of decimal numbers. In addition, as for the field of I1-I5, information is recorded by 6 bits, and, as for the field of I6-I12, information is recorded by 4 bits.

Moreover, drawing 35 is drawing showing a format of the ISRC data which drive equipment read, and a serial number is written in the field of I8-I12 shown in this drawing 35 with the decimal number for 5 figures.

[0023] Drawing 38 is drawing showing the 3rd example of data logging. As shown in this drawing 38 , it is recorded by the mode dimorphism formula between mode 1 formats of a Q channel field, and is further recorded also in mode 3 format. Moreover, MCN (for example, 1234567890123) is written in the data of the mode dimorphism type in that case, and the serial number of ISRC is 98765 in the data of mode 3 format. It is written in.

[0024] As mentioned above, CD-R/RW is standardized and is excellent in compatibility, and the contents of a format deal with it very much, and tend to carry out it. However, since a user individual can reproduce works, such as music and data of a movie or a computer program, easily, this CD-R/RW has the technical problem that protection of such a work is not thoroughgoing.

[0025] The approach of protecting such data with copyright has the approach of adding dues to sound recording / playback device beforehand, the approach of performing to the data stream when copying by putting coding information, etc. However, the approach of the approach of adding dues beforehand having the technical problem that a setup of a tariff is very difficult, and putting coding information on the data stream when copying has the technical problem that

there are no means prevented in any way in copying in analog, and neither serves as fundamental solution for duplicate prevention.

[0026] In addition, about data logging, as shown below, four kinds of well-known reference is known. First, the distinction means of CD-ROM which equips JP,8-153331,A (the well-known reference 1 may be called hereafter) with the DS in which a copy protection is possible, and copy article CD-ROM is acquired, and the technique of aiming at prevention of an illegal copy is indicated.

[0027] However, the technique indicated by this well-known reference 1 makes the particular part of a medium the specific value for anti-copying. Furthermore, since this technique makes the specific value Q channel address of a sub-code block of the arbitration of CD, it has the technical problem that the dependability of data protection is low. Moreover, the technique of performing anti-copying of the recorded software or music information is indicated, without carrying out the cost rise of the optical disk which supplies software and music information to JP,7-85574,A (the well-known reference 2 being called hereafter).

[0028] The technique indicated by this well-known reference 2 has prevented the copy by recording the key information on encryption on a non-data storage area by a bar code etc. However, a non-data area is a field which the optical head of a regenerative apparatus does not scan, and since key information is recorded by the bar code or the geometrical pattern, it has the technical problem that the key

information reading means of dedication is required.

[0029] Furthermore, it is media, such as CD-ROM on which data were recorded in the pit, and even if the duplicate of a metaphor pit formation part is made without being reproduced simply, the data-logging medium which can be prevented from reproducing easily the information signal currently recorded is indicated by USP5,802,174 (Japanese corresponding application may call the well-known reference 3 JP,9-017119,A and the following).

[0030] The technique indicated by this well-known reference 3 records encryption data and cryptographic key information on two record sections where a record format differs from a recording layer separately, and cryptographic key information is recorded by the wobble and the optical MAG of a slot, or the phase change, or it records them on other recording layers. However, since each ****** is an anti-copying technique of a ROM medium, such as CD-ROM, application to a recordable medium like this invention is difficult to even indicate for this well-known reference 3.

[0031] Furthermore, reading and the copy of a cryptographic key will be easily made only by changing the recording layer which writes in a cryptographic key. When cryptographic key information is written in by the wobble of a slot, a different identification number for every disk cannot be given, but there is no anti-copying effectiveness in a recordable medium. Moreover, when

cryptographic key information is written in using other record formats other than pits, such as optical MAG, in order to read, the technical problem that the key information reading means of dedication is required occurs.

[0032] And the data recorder unreproducible even if reproduced is indicated by EP751516A (Japanese corresponding application may call the well-known reference 4 JP,9-115241,A and the following), without being reproduced simply. However, the technique indicated by this well-known reference 4 records the identification information of a proper on a medium, and that identification information is recorded on a data area, a TOC field, etc. Therefore, since a TOC field is rewritten by the user at arbitration, it has too the technical problem that there is fear of an alteration of the data encryption key by the user.

[0033]

[Problem(s) to be Solved by the Invention] This invention by having been originated in view of such a technical problem, and giving predetermined initialization to a disk using the existing format approach Although a user is able to copy the data with copyright of music, the data of a movie or a computer program, etc. to the disk of one sheet only once It aims at offering sound, an image, and a data station in a decryption equipment list at the encryption approach on a record medium, and an encryption equipment list in the initialization approach list of a record medium and a record medium which

cannot be secondarily copied to other disks from the copied disk.

[0034]

[Means for Solving the Problem] For this reason, the record medium of this invention is the field which can read a reader, a user offers the management domain which cannot access that field, and the data area where it is the field which a reader can read and a user can access that field at arbitration, and it is characterized by recording the disk identification information for encryption on that management domain (claim 1).

[0035] Moreover, media information including voice, an image, and any one information on the data to the data area While being recorded as encryption media information enciphered by the cryptographic key generated using the above-mentioned disk identification information at least The medium identification number information which a user can read may be distributed and recorded, and this record medium may be made to be recorded on optical, and a user may be made for that data area to be written in once [at least] (claims 2-4).

[0036] In addition, this encryption Even if it is made to be carried out using the information which combined the serial number information or these which were recorded on the frame of mode 3 format of a Q channel sub-code by the medium identification number information list recorded on the frame of the mode dimorphism type of disk identification information and a Q channel sub-code

Often (claim 14) The random-number function which uses as a seed information which combined the serial number information or these which were recorded on the medium identification number information list recorded on the frame of the mode dimorphism type of disk identification information and a Q channel sub-code by the frame of mode 3 format of a Q channel sub-code It may be made to be carried out by using (claim 15). Bit length The serial number information or these which were recorded on the medium identification number information list recorded on the frame of the mode dimorphism type of the key message in which is changed and it deals, disk identification information, and a Q channel sub-code by the frame of mode 3 format of a Q channel sub-code It may be made to be carried out using the Hash Function which uses combined information as a seed (claim 16).

[0037] Furthermore, the initialization approach of the record medium of this invention is the field which can read a reader, and a user is the initialization approach of a record medium of having offered the management domain which cannot access the field, and the data area where it is the field which a reader can read and a user can access the field at arbitration, and is characterized by recording the disk identification information for encryption on a management domain (claim 5).

[0038] And in recording the above-mentioned disk identification information, the

1st write-in step which records the disk identification information for encryption on a management domain, the 2nd write-in step which records medium identification number information by the mode dimorphism formula of a Q channel sub-code in a data area, and the 3rd write-in step which records serial number information in mode 3 format of a Q channel sub-code in a data area are offered, and it may be constituted (claim 6).

[0039] In addition, this encryption Even if it is made to be carried out using the information which combined the serial number information or these which were recorded on the frame of mode 3 format of a Q channel sub-code by the medium identification number information list recorded on the frame of the mode dimorphism type of disk identification information and a Q channel sub-code Often (claim 17) The random-number function which uses as a seed information which combined the serial number information or these which were recorded on the medium identification number information list recorded on the frame of the mode dimorphism type of disk identification information and a Q channel sub-code by the frame of mode 3 format of a Q channel sub-code It may be made to be carried out by using. Again Bit length The serial number information or these which were recorded on the medium identification number information list recorded on the frame of the mode dimorphism type of the key message in which is changed and it deals, disk identification information, and a Q channel

sub-code by the frame of mode 3 format of a Q channel sub-code It may be made to be carried out using the Hash Function which uses combined information as a seed.

[0040] In addition, the encryption approach on the record medium of this invention The management domain where it is the field which a reader can read and a user cannot access the field, It is the field which a reader can read and is the encryption approach on the record medium with which the user offered the data area which can access the field at arbitration. After performing initialization which records the disk identification information for encryption on a management domain By enciphering by the cryptographic key using the above-mentioned disk identification information at least, and recording media information including voice, an image, and any one information on the data on a data area as encryption media information It is characterized by having offered the encryption step which generates a specific record medium, and being constituted (claim 7).

[0041] And the above-mentioned initialization may consist of a 1st write-in step which records the disk identification information for encryption on a management domain, a 2nd write-in step which records medium identification number information on a data area by the mode dimorphism formula of a Q channel sub-code, and a 3rd write-in step which records serial number information on a data area in mode 3 format of a Q channel sub-code (claim 8).

[0042] Moreover, the 1st disk identification information read-out step from which the encryption step reads disk identification information as the 1st disk identification information, The 1st cryptographic key generation step which generates the 1st cryptographic key combining the 1st disk identification information and at least one information in medium identification number information and serial number information, The 1st read-out step which reads media information from an external device, and by generating encryption media information using the 1st cryptographic key, and recording on the data area which has the 1st disk identification information The specific record-medium generation step which generates a specific record medium is offered, and it may be constituted (claim 9).

[0043] In addition, this encryption may be made to be performed using disk identification information and the information which combined serial number information or these with the medium identification number information list (claim 18). It may be made to be carried out using the random-number function which uses as a seed disk identification information and information which combined serial number information or these with the medium identification number information list (claim 19). Moreover, it may be made to be carried out using the Hash Function which uses as a seed the key message in which bit length is changed and it deals, disk identification information, and information which

combined serial number information or these with the medium identification number information list (claim 20).

[0044] Furthermore, the management domain where the encryption equipment of this invention is the field which can read a reader, and a user cannot access the field, The data area where it is the field which a reader can read and a user can access the field at arbitration is offered. The read-out means which can read at least the disk identification information in the record medium with which the disk identification information for encryption was recorded on the management domain, The encryption media information generation means which enciphers media information including voice, an image, and any one information on the data to a data area, and may be outputted to it as encryption media information by the cryptographic key using the above-mentioned disk identification information at least, It is characterized by having offered an encryption media information preservation means by which encryption media information could be saved in the data area of the record medium which has the same disk identification information, and being constituted (claim 10).

[0045] In addition, this encryption It may be made to be carried out using the information which combined the serial number information or these which were recorded on the frame of mode 3 format of a Q channel sub-code by the medium identification number information list recorded on the frame of the mode

dimorphism type of disk identification information and a Q channel sub-code. The random-number function which uses as a seed information which combined the serial number information or these which were recorded on the medium identification number information list recorded on the frame of the mode dimorphism type of disk identification information and a Q channel sub-code by the frame of mode 3 format of a Q channel sub-code It may be made to be carried out by using. Again Bit length The serial number information or these which were recorded on the medium identification number information list recorded on the frame of the mode dimorphism type of the key message in which is changed and it deals, disk identification information, and a Q channel sub-code by the frame of mode 3 format of a Q channel sub-code It may be made to be carried out using the Hash Function which uses combined information as a seed.

[0046] And the management domain where the decryption equipment of this invention is the field which can read a reader, and a user cannot access the field, While offering the data area where it is the field which a reader can read and a user can access the field at arbitration and recording the disk identification information for encryption on a management domain The 2nd read-out means which can read at least the disk identification information in the record medium with which the information enciphered by the data area was recorded, A 2nd

cryptographic key generation means to generate the 2nd cryptographic key from disk identification information at least, The enciphered information is decoded using the 2nd cryptographic key, and it is characterized by having offered the decryption means which can reproduce media information including voice, an image, and any one information on the data, and being constituted (claim 11).

[0047] In addition, this encryption It may be made to be carried out using the information which combined the serial number information or these which were recorded on the frame of mode 3 format of a Q channel sub-code by the medium identification number information list recorded on the frame of the mode dimorphism type of disk identification information and a Q channel sub-code. The random-number function which uses as a seed information which combined the serial number information or these which were recorded on the medium identification number information list recorded on the frame of the mode dimorphism type of disk identification information and a Q channel sub-code by the frame of mode 3 format of a Q channel sub-code It may be made to be carried out by using. Again Bit length The serial number information or these which were recorded on the medium identification number information list recorded on the frame of the mode dimorphism type of the key message in which is changed and it deals, disk identification information, and a Q channel sub-code by the frame of mode 3 format of a Q channel sub-code It may be

made to be carried out using the Hash Function which uses combined information as a seed.

[0048] In addition, the sound, image, and data station of this invention The management domain where it is the field which a reader can read and a user cannot access the field, The data area where it is the field which a reader can read and a user can access the field at arbitration is offered. The read-out means which can read at least the disk identification information in the record medium with which the disk identification information for encryption was recorded on the management domain, The encryption media information generation means which enciphers media information including voice, an image, and any one information on the data, and may be outputted as encryption media information by the cryptographic key using disk identification information at least, It is characterized by having offered an encryption media information preservation means by which encryption media information could be saved in a data area, and being constituted (claim 12).

[0049] Moreover, the management domain where the sound, image, and data station of this invention are the fields which can read a reader, and a user cannot access the field, While offering the data area where it is the field which a reader can read and a user can access the field at arbitration and recording the disk identification information for encryption on a management domain The 2nd

read-out means which can read at least the disk identification information in the record medium with which the information enciphered by the data area was recorded, A 2nd cryptographic key generation means to generate the 2nd cryptographic key from disk identification information at least, The enciphered information is decoded using the 2nd cryptographic key, and it is characterized by having offered the decryption means which can reproduce media information including voice, an image, and any one information on the data, and being constituted (claim 13).

[0050] In addition, this encryption It may be made to be carried out using the information which combined the serial number information or these which were recorded on the frame of mode 3 format of a Q channel sub-code by the medium identification number information list recorded on the frame of the mode dimorphism type of disk identification information and a Q channel sub-code. The random-number function which uses as a seed information which combined the serial number information or these which were recorded on the medium identification number information list recorded on the frame of the mode dimorphism type of disk identification information and a Q channel sub-code by the frame of mode 3 format of a Q channel sub-code It may be made to be carried out by using. Again Bit length The serial number information or these which were recorded on the medium identification number information list

recorded on the frame of the mode dimorphism type of the key message in which is changed and it deals, disk identification information, and a Q channel sub-code by the frame of mode 3 format of a Q channel sub-code It may be made to be carried out using the Hash Function which uses combined information as a seed.

[0051]

[Embodiment of the Invention] Hereafter, CD-R/RW is made into an example, and the gestalt of operation of this invention is explained with reference to a drawing.

(A) The explanatory view 1 of the 1st operation gestalt of this invention is drawing showing arrangement with the non-data area of CD-R/RW where this invention is applied, and a data area. The disk 10 shown in this drawing 1 is a record medium in which read-out or writing is possible, and has offered the management domain 11 and the user area 12 on optical. Moreover, this disk 10 is the thing before being initialized.

[0052] Here, what Disks ID and MCN, ISRC, etc. are inserted in a disk (a disk or media may be called) with physical initialization for (it records) is said. Moreover, the mode which uses the initialized disk has industrial use and a noncommercial use. That is, industrial use means for example, a primary manufacturer initializing and selling to this physical disk, and a secondary manufacturer

purchasing that initialized physical disk, and recording and selling voice, an image, data, etc. Moreover, a noncommercial use means purchasing the disk by which the consuming public was initialized and recording voice, an image, data, etc. on individual level. Therefore, the word of a user means the secondary manufacturer, a consuming public, etc. hereafter. In addition, specifically, this disk 10 is CD-R which can be written in only once, or rewritable CD-RW of data repeatedly.

[0053] This management domain 11 is a field which drive equipment (not shown) can read, and a user is the field which cannot access that field and it consists of PCA and PMA. Here, drive equipment is a reader in the regenerative apparatus of CD-R/RW, or a recording device. Namely, although the drive equipment built in the noncommercial regenerative apparatus which a user uses can read this management domain 11, a user can rewrite the value of this management domain 11 to arbitration, or can eliminate it no longer. That is, it is the field where the command for a user rewriting to arbitration or eliminating does not exist. Moreover, PCA is a field where the information for adjusting the strength of the laser when writing in data is recorded.

[0054] Furthermore, PMA is a field where the disk ID for encryption (disk identification information) is recorded, and each disk is identified with this disk ID. Moreover, in case it initializes a disk, by drive equipment, this disk ID sets up a

number almost at random, is not written in, and unless it is still more nearly special equipment, it cannot set this disk ID as a specific number. Therefore, since the user who uses it in a home or office does not have such special equipment, a specific number rewrites this disk ID.

[0055] In addition, one management domain 11 is usually established in the most inner circumference, and capacity is 1% or less of data-logging capacity very few. Furthermore, a user area 12 is a field which drive equipment can read, and is a field where a user can access the field at arbitration. This user area 12 consists of lead-in groove field 12a for storing a lead-in groove, data area (program field) 12b for storing data, such as music, and lead-out field 12c for storing lead-out.

[0056] And multimedia data, such as voice, an image, and data To this data area 12b, Disks ID and MCN (medium identification number information), While being enciphered by the cryptographic key (cryptographic key) generated using the serial number (serial number information) of ISRC and being recorded as encryption data (encryption media information) The serial number of MCN and ISRC which a user can read is distributed and recorded on this data area 12b. That is, in case a user writes in music data, data, such as a movement number of a silent part and music, an index, time amount, and an alphabetic character, are written in the field for subcoding in data area 12b with music data. In addition,

data area 12b of CD-R is written in once by the user, and data area 12b of CD-RW can be rewritten any number of times by the user.

[0057] Here, MCN is the identifier of a media number and is the information recorded by Q channels (mode dimorphism type) of the field for the subcoding. Furthermore, the serial number of ISRC is the information recorded by Q channels (mode 3 format) of the field for subcoding. Drawing 2 (a) is drawing showing notional field arrangement of CD-R/initialized RW. The disk 10 shown in this drawing 2 (a) has data area 12b and the media number field 1. In addition, the hole of the core of a disk 10 is omitted.

[0058] Here, the media number field 1 is a notional field which gathered up the above-mentioned disks ID and MCN and three fields of ISRC, in fact, it is not such a form and the field of a disk 10 is not necessarily used. Moreover, Disk ID is 6 figures of a decimal number, MCN is 13 figures of decimal numbers, the serial number of ISRC is 5 figures of decimal numbers, these are put together suitably and such die length is used as a cryptographic key. In addition, about the combination, it mentions later.

[0059] And multimedia data are enciphered by these stenciled disks ID and MCN and the media number which combined the serial number of ISRC. Or the whole ISRC may be used instead of the serial number of ISRC. Drawing 2 (b) is drawing showing notional field arrangement of CD-R/RW on which encryption

data were recorded, and, as for disk 10' shown in this drawing 2 (b), the media number field 1 and the encryption data 14 are recorded. That is, multimedia data are enciphered using a media number as a cryptographic key, and the encryption data 14 shown in drawing 2 (b) are obtained.

[0060] Drawing 3 is drawing for explaining being enciphered by the media number. The data 13 (circular thing on the left-hand side of drawing 3) shown in this drawing 3 are data which are not enciphered, and, specifically, are multimedia data including the information on voice, an image, data, etc. And this data 13 is enciphered by the cryptographic key using Disks ID and MCN and the media number (media number field) 1 which it becomes from the serial number of ISRC, and as shown in this drawing 3 , the encryption data 14 (circular thing on the right-hand side of drawing 3) are obtained. Furthermore, what this encryption data 14 was recorded on is generated as specific disk 10' (encryption step). That is, since the media number (media number field) 1 is a different peculiar thing for every one disk, it is functioning as a cryptographic key.

[0061] Therefore, the encryption approach on the record medium of this invention The management domain 11 where it is the field which drive equipment (illustration abbreviation) can read, and a user cannot access the field, It is the field which drive equipment can read and is the encryption approach on the disk 10 with which the user offered data area 12b which can

access the field at arbitration. After performing initialization which records the disk ID for encryption on a management domain 11 By enciphering by the code key using the above-mentioned disk ID, and recording media information including voice, an image, and any one information on the data on data area 12b as encryption media information It means that the encryption step which generates specific disk 10' is offered, and it was constituted.

[0062] Here, the above-mentioned initialization consists of the 1st write-in step which records the disk ID for encryption on a management domain 11, the 2nd write-in step which records Disks ID and MCN (medium identification number information) on data area 12b by the mode dimorphism formula of a Q channel sub-code, and the 3rd write-in step which records the serial number (serial number information) of ISRC on data area 12b in mode 3 format of a Q channel sub-code so that it may mention later using drawing 8 .

[0063] Specifically, as for this encryption step, Disk ID is first read as the 1st disk identification information (the 1st disk identification information read-out step). Furthermore, the media number 1 is generated in combination with the disks ID and MCN, combination with the serial number of Disks ID and ISRC, or the combination of Disks ID and MCN and the serial number of ISRC (the 1st cryptographic key generation step). And specific disk 10' is generated by reading data 13 from an external device (the 1st read-out step), generating the

encryption data 14 using the media number 1, and being recorded on data area 12b of a disk 10 which has the same disk ID (specific record-medium generation step).

[0064] Drawing 4 is drawing for explaining being decrypted by the media number. The encryption data 14 shown in this drawing 4 are decoded by media number (media number field) 1' (restoration), and the original data 13 are obtained. Namely, as for a decryption step, the disk ID of specific disk 10' is first read as the 2nd disk identification information. And the encryption data 14 are read from this specific disk 10', and media number (media number field) 1' is generated from combination with those disks ID and MCN, combination with the serial number of Disks ID and ISRC, and the combination of Disks ID and MCN and the serial number of ISRC. That is, media number (media number field) 1' is functioning as the 2nd cryptographic key. Here, only when media number 1' is in agreement with the media number 1, the encryption data 14 are decoded and can be reproduced.

[0065] Drawing 5 is drawing for explaining that a secondary copy is not made. Two kinds of different things of disk 10' and disk 10a are shown in drawing 5 . Here, disk 10' is the disk primarily copied for example, from the music CD. On the other hand, disk 10a is initialized another disk, and is further copied secondarily from disk 10' copied primarily.

[0066] Here, since the media number 1 and media number 1' which are a cryptographic key differ from each other even if it reads the data copied secondarily by CD-R / RW drive (after-mentioned), the encryption data 14 of this copied disk 10a are not decoded. Thus, since the cryptographic key using a media number becomes a general way, a secondary copy is prevented. Moreover, the data used as a cryptographic key are distributed and recorded on these fields in this way using the management domain 11 in a CD-R disk or a CD-RW disk, and data area 12b, the data distributed and recorded is gathered up, and the cryptographic key is generated. Therefore, according to this approach, it can encipher now, without changing the format approach of the existing disk. in addition, since the distributed approach can be made to change into versatility if needed, it can raise the reinforcement as a cryptographic key.

[0067] Next, the media number which is a cryptographic key is explained concretely. There is an asymmetry method which is not the same in the encryption approach as known well. The example using the former has DES (Data Encryption Standard), RC4 (Rivest Code #4), IDEA, etc., and the example using the latter has RSA (Rivest, Shamit, and Adleman) etc.

[0068] Drawing 6 is drawing showing the encryption approach which used the cryptographic key. Data "ABCD" of origin has " cryptographic key " multiplied as shown in this drawing 6 , and it is encryption data ". ?" is obtained. And

encryption data ". ?" has "decryption key " multiplied, and the original data "ABCD" are obtained. And for DES, 56 bits and RC4 are [46-128 bits and IDEA of the die length of the cryptographic key usually used] 128 bits, respectively, and RSA is 512-4096 bits. In addition, this 56 bits DES and 1024-bit RSA have the comparable difficulty of that decode.

[0069] By the way, when enciphering using the above-mentioned media number, the media number must have a number required for the encryption of bits. On the other hand, MCN is 13 figures (binary number of 43.2 bits) of decimal numbers, and ISRC is 5 figures (binary number of 16.6 bits) of decimal numbers, and Disk ID is 6 figures (binary number of 19.9 bits) of decimal numbers. The code of sufficient die length cannot be created in these simple substances. Therefore, according to the encryption approach which uses these three kinds, three kinds of above-mentioned cryptographic keys 1-3 are combined. Next, the example of use of cryptographic keys 1-3 is shown in (vi) from (i). In addition, in the following explanation, a cryptographic key 1 and the serial number of ISRC may be called a cryptographic key 2, Disk ID may be called a cryptographic key 3, and MCN may be explained.

(i) When 6 figures of decimal numbers are enough as the die length of a cryptographic key, a cryptographic key 3 (6 figures of decimal numbers) is used.

(ii) When 11 figures of decimal numbers are enough as the die length of a

cryptographic key, a cryptographic key 2 (5 figures of decimal numbers) and a cryptographic key 3 (6 figures of decimal numbers) are used.

(iii) When 19 figures of decimal numbers are enough as the die length of a cryptographic key, a cryptographic key 1 (13 figures of decimal numbers) and a cryptographic key 3 (6 figures of decimal numbers) are used.

(iv) When 24 figures of decimal numbers are enough as the die length of a cryptographic key, a cryptographic key 1 (13 figures of decimal numbers), a cryptographic key 2 (5 figures of decimal numbers), and a cryptographic key 3 (6 figures of decimal numbers) are used.

(v) When the die length of a cryptographic key is larger than (iv), a cryptographic key 1, a cryptographic key 2, and a cryptographic key 3 are resembled, in addition only the cryptographic key which a part for data division runs short of is created and used. For example, from one of suitable format parts, in the case of the 30-figure need, you may acquire other 6 figures, or it may also write the 6 figures in a part for data division.

(vi) It is the case that the die length of a cryptographic key is larger than (iv), and when it is a CD-R disk, by creating two or more trucks, two or more cryptographic keys 1 and cryptographic keys 2 are created, respectively, and the cryptographic keys 1 and 2 of these plurality and a cryptographic key 3 are used collectively.

[0070] Moreover, the secrecy nature of a cryptographic key must be raised in a data encryption. In that case, it is calculated by three kinds of the serial number (cryptographic key 2) of MCN (cryptographic key 1) and ISRC and Disk ID (cryptographic key 3) being substituted for a specific function, respectively, and the calculated result is used as a cryptographic key. In order to be adopted as this specific function, the conditions of ** of a degree and ** need to be fulfilled.

[0071] ** The same result should be obtained from the serial number of the same MCN and ISRC, and Disk ID.

** Reverse analysis should be hard to be carried out.

The conditions of this ** are because a result different each time appears and it becomes impossible to reproduce a fixed cryptographic key, when the function which generates a true random number is used. Moreover, the conditions of ** are because the original MCN, the serial number of ISRC, and Disk ID are not decoded from the calculated result using an inverse function, respectively. These three kinds of cryptographic keys are called ID for convenience, and the algorithm which generates a cryptographic key is explained using drawing 39 (a) - (c).

[0072] It is the explanatory view of the cryptographic key generation method with which drawing 39 (a) is the explanatory view of the cryptographic key generation method which carried out simple addition of three kinds of cryptographic keys

1-3, and the random-number function was used for drawing 39 (b) for three kinds of cryptographic keys 1-3, respectively, and drawing 39 (c) is the explanatory view of the cryptographic key generation method which used the Hash Function for a key message and three kinds of cryptographic keys 1-3. In addition, in these drawings, a cryptographic key is displayed also as unique ID, and ID1 and a cryptographic key 2 (serial number of ISRC) are displayed as ID2, and the cryptographic key 3 (disk ID) is displayed for the cryptographic key 1 (MCN) as ID3, respectively.

[0073] Here, it is equivalent to (iv) mentioned above - (vi), and three kinds of things, a cryptographic key 1 (ID1), a cryptographic key 2 (ID2), and a cryptographic key 3 (ID3), are added, and, as for Case1 shown in drawing 39 (a), a cryptographic key (unique ID) is generated. Moreover, when the die length of a required cryptographic key is short, it is equivalent to (i) mentioned above - (iii), and the serial number of MCN and ISRC and Disk ID may be used according to an individual. Therefore, this encryption will be performed using the information which combined Disks ID and MCN, the serial number of ISRC, or these. And six kinds of the way of combining exists from three kinds of the serial number of MCN and ISRC, and Disk ID.

[0074] Next, the result of the random-number function Rnd (ID1) with which the cryptographic key (unique ID) generated MCN (ID1) as a seed in Case2 shown

in drawing 39 (b), The result of the random-number function Rnd (ID2) which generated the serial number (ID2) of ISRC as a seed, and the result of the random-number function Rnd (ID3) which generated Disk ID (ID3) as a seed are added, and are obtained.

[0075] Here, random-number function Rnd() is a function which generates a pseudo-random number based on the inputted kind, and to the number inputted as a seed, this random-number function Rnd() carries out the multiplication of the very large integer, adds a very large integer to that multiplication result, and outputs the value in the predetermined digit of that addition result further. Moreover, a seed means the initial value for performing the random-number-generation operation inside the random-number function Rnd().

[0076] Therefore, it will mean that this encryption was made using the random-number function which uses Disks ID and MCN or the serial number of ISRC as a seed, and this encryption will be made using the random-number function which uses as a seed information which combined Disks ID and MCN or the serial number of ISRC. Random-number function Rnd() prepares the table of random numbers of immobilization beforehand, and outputs a specific figure to the serial number of the same MCN and the same ISRC, and the same disk ID so that the same result may be outputted, when generating a cryptographic key practically using the serial number of the same MCN and the same ISRC, and

the same disk ID. In addition, the serial number of MCN and ISRC and three kinds of all of Disk ID are added, and you may make it substitute for random-number function Rnd() by using the addition result as a seed.

[0077] Thus, in an algorithm, since random-number function Rnd() is used, the same cryptographic key comes to be outputted and reverse analysis is hard, as for the generated cryptographic key, to be carried out. In addition, in Case3 shown in drawing 39 (c), the cryptographic key (unique ID) is generated by the approach of calculating and obtaining a variable-length key message, MCN (ID1), the serial number (ID2) of ISRC, and the thing adding Disk ID (ID3) by the Hash Function.

[0078] Here, a Hash Function is a function which considers the text (text data) of predetermined length as an input, and considers a fixed-length message digest (message digest data) as an output. In addition, it may be called a message digest also with a hash value. Moreover, in the following explanation, the text of this predetermined length is equivalent to what divided into suitable die length what should mean the 128-bit disk ID etc. and specifically combined Disk ID etc., and was obtained. And bit length inputted is made not only into 128 bits but into 80 bits, or is made to 200 bits. That is, although the burden of encryption processing and decryption processing mitigates when short, safety is no longer collateralized. On the contrary, safety is collateralized, although the burden of

encryption processing and decryption processing increases when long. That is, this bit length is changed by the design plan and it deals in it.

[0079] Moreover, when the serial number of MCN and ISRC and the thing which added Disk ID altogether do not fulfill 128 bits, after a bit string (key message) is added to the serial number of MCN and ISRC, and the thing adding Disk ID and being made 128 bits, the operation by the Hash Function is performed. Furthermore, you may make it software (driver software) insert a fixed message automatically, or a user may be made to insert about a key message. Moreover, the key message according to the class of information to record may be made to be added. And in order to raise the safety of a cryptographic key, a key message is made not to be recorded on the same disk as the disk with which Disk ID is recorded.

[0080] Therefore, this encryption will be performed using the Hash Function which uses as a seed the key message and Disks ID and MCN in which bit length is changed and it deals, or the serial number of ISRC, and this encryption will be performed using the Hash Function which uses as a seed information which combined a key message, Disks ID and MCN, or the serial number of ISRC.

[0081] Next, the class of Hash Function of this Case3 is explained using a concrete example program. As mentioned above, a hash algorithm has a thing

of ISRC, the probability for the same cryptographic key to be generated becomes very small.

[0084] By using these MD methods, the magnitude of a message digest can be changed easily and software processing using CPU which is 32 bits or 64 bits is performed at a high speed. On the other hand, a hash algorithm has an algorithm called others, RIPEMD, and SHA. [method / these / MD] This RIPEMD is an algorithm which generates a 160-bit message digest. Moreover, SHA-1 is the algorithm which improved MD4, SHA can generate the message digest of 160 bit length longer than MD4 and MD5 from the text of arbitration length, and it is prescribed by FIPS 180-1.

[0085] Drawing 40 is drawing showing the example program of a Hash Function. Function func() shown in this drawing 40 has the algorithm of the best Hash Function (the best Hash Function), an input variable is (*str) of a pointer, and an output is a message digest (val%SIZE). And other functions (illustration abbreviation), such as the Maine function, pass the pointer (*str) which expresses the head location of the bit string of predetermined length to this function func(), and call function func(). And a hash value val is calculated by the die length of the inputted bit string of a predetermined number being found in len=strlen (str). This val is the value of triple figures expressed with the number of 26 **, and at least that of 1 of a decimal number is equivalent at least to that of

100 at least for that of 10, respectively. *str-'a' expresses the head of an input string, *(str+len/2)-'a' expresses the center section of the input string here, and it is * (str+ (len-1)) further. - 'a' expresses the tail end of an input string. And the division of this outputted val is done by SIZE (for example, 1023), and it is classified into 1023 kinds of remainders. Thereby, all the inputted alphabet trains are permuted by 1023 kinds of message digests. In addition, when a pointer variable is 0 (NULL), 0 is outputted, without performing the operation of a hash algorithm.

[0086]

[Table 1]

ハッシュ関数を用いた計算の実行条件の一例

サイズ:1023
繰り返し回数:10

データ総数(個)	挿入時間(秒)	検索時間(秒)	削除時間(秒)	要素数の平均	要素数の最大値	要素数の最小値
50000	1.5850	2.6950	1.6550	35.266	54.400	23.000

[0087]

[Table 2]

ハッシュ関数により生成されたデータの分布の一例

ハッシュ値の範囲	生成されたデータ個数(1つの＊は50の要素数に相当)
table[0 ～ 49]:	********************************** 1922
table[50 ～ 99]:	********************************** 1930
table[100 ～ 149]:	********************************** 1904
table[150 ～ 199]:	********************************** 1968
table[200 ～ 249]:	********************************** 1765
table[250 ～ 299]:	********************************** 1834
table[300 ～ 349]:	********************************** 1836
table[350 ～ 399]:	********************************** 1781
table[400 ～ 449]:	********************************** 1749
table[450 ～ 499]:	********************************** 1876
table[500 ～ 549]:	********************************** 1707
table[550 ～ 599]:	********************************** 1747
table[600 ～ 649]:	********************************** 1756
table[650 ～ 699]:	********************************** 1738
table[700 ～ 749]:	********************************** 1806
table[750 ～ 799]:	********************************** 1768
table[800 ～ 849]:	********************************** 1753
table[850 ～ 899]:	********************************** 1840
table[900 ～ 949]:	********************************** 1778
table[950 ～ 999]:	********************************** 1806
table[1000 ～ 1022]:	********** 850

ヒストグラム平均:1813.978495
平均:36.279570
最大値:57
最小値:21

[0088] As it is the table showing the execution condition of the count which used the Hash Function and is shown in this table 1, the number of Tables 1 is 50000, and they repeat the number of data (data total) inputted 10 times. Furthermore, Table 2 is a table showing an example of distribution of the data generated by the Hash Function, table expresses the range of a message digest value (hash value), and * expresses the histogram (generated data number) of the range. Here, the number of elements contained in one * is 50. For example, it is the

[0091] Moreover, when decoding in regular-user level about secrecy nature using a personal computer, it is next to impossible to decode a 128-bit message digest in the number of the bus lines of CPU and the number of bits of memory which are carried in the personal computer. Therefore, a user cannot carry out the secondary copy of the data with copyrights, such as music, a movie, and a computer program, in practice, but this data with copyright is protected.

[0092] Thus, the number of bits required for encryption is secured also with a user's drive equipment by PMA which can be read, and MCN and ISRC which were distributed by data area 12b and recorded on it. Drawing 7 is the mimetic diagram of the cryptographic key imprinting equipment concerning the 1st operation gestalt of this invention. The cryptographic key imprinting equipment 19 shown in this drawing 7 enciphers multimedia data, such as voice, an image, and data, records them as encryption data, offers a personal computer 20, a cable 43, and CD-R / RW drive 46, and is constituted. Moreover, CD-R disk (CD-R media) 47a or CD-RW disk (CD-RW media) 47b is a disk before initialization (media).

[0093] This personal computer 20 performs initialization of CD-R disk 47a or CD-RW disk 47b, offers the media number setting means 45, and is constituted. This media number setting means 45 is Mode Select so that the value of the serial number of MCN and ISRC may be set up and the value which those who

operate it inputted can be kept temporarily. It has the memory for commands (not shown). Moreover, this personal computer 20 is UDF (Universal Disk Format) which is a logical format in the case of initialization of a disk. It gives.

[0094] In case a user copies this personal computer 20, it can perform the logical format corresponding to the software (for example, trade name of DirectCD;Adaptec) which a user uses. Here, with DirectCD, in case a user copies, it is the software for writing it was made to be possible [whose handling] in the environment same with treating the file which is contained in the integral disk or the floppy disk in the file included in CD-R / RW drive 46.

[0095] And in case a disk is initialized, a user performs a logical format using DirectCD. Moreover, a user is ISO9660. It is ISO9660 when you want to take transposition. A logical format can also be added and it is ISO9660 in that case. It is necessary to perform two kinds in all of formats with DirectCD. This ISO9660 (Internatinal Organization for Standardization 9660) It is an international standard and CD-ROM or the file in CD-R/RW, directory structure, a logical format, etc. are defined. Moreover, ISO9660 It is an extensible specification and various extended specifications are specified. Furthermore, ISO9660 There is an information-interchange level and it defines from level 1 to level 3. In addition, generally it is ISO9660. Level 1 is then pointed out. The alphabetic character which this can use, and the specification of use of a file name are contained.

[0096] In addition, although this personal computer 20 has other well-known functions, it omits that detailed explanation. And a cable 43 connects electrically a personal computer 20, and CD-R / RW drive 46. Moreover, CD-R / RW drive 46 records the above-mentioned disks ID and MCN and the serial number of ISRC on the inserted disk.

[0097] Thereby, in the media number setting means 45 of the personal computer 20 in cryptographic key imprinting equipment 19, the serial number of MCN and ISRC is set up and the set-up value is inputted into CD-R / RW drive 46 through a cable 43. And in this CD-R / RW drive 46, while the serial number of MCN and ISRC is recorded, Disk ID is recorded automatically.

[0098] Initialization for the anti-copying of CD-R/RW is performed by such configuration. The initialization flow of CD-RW and CD-R is explained using drawing 11 from drawing 8 . Drawing 8 is an initialization flow chart in the anti-copying approach of CD-RW concerning the 1st operation gestalt of this invention.

[0099] The initialization approach of the record medium of this invention is the field which drive equipment (illustration abbreviation) can read, and users are the management domain 11 which cannot access the field, and the field which drive equipment can read, are the initialization approaches of a record medium (disk 10) that the user offered data area 12b which can access the field at

arbitration, and record the disk ID for encryption on the management domain 11.

[0100] As for the initialization step started from step A1, in step A2, CD-RW disk (CD-RW media) 47b is first inserted in CD-R / RW drive 46. And it sets to step A3 and is Mode Select. The memory for commands (not shown) is secured, it sets to step A4 further, and a cryptographic key 1 is Select. It is set as the memory for commands, it sets for step A5, and a cryptographic key 2 is Select. It is set as the memory for commands. And it sets to step A6 and is Mode Select. By publishing a command, these cryptographic keys 1 and a cryptographic key 2 are prepared.

[0101] Here, in step A7, the Format command is published, and a cryptographic key 1 and a cryptographic key 2 are actually written in data area 12b, and a cryptographic key 3 is written in a management domain 11. That is, MCN is recorded on data area 12b by the mode dimorphism formula of a Q channel sub-code (the 2nd write-in step), and the serial number of ISRC is recorded on it in mode 3 format of a Q channel sub-code (the 3rd write-in step).

[0102] In addition, this cryptographic key 3 is automatically published by CD-R / RW drive 46, and the disk ID for encryption is recorded on the above-mentioned management domain 11 (the 1st write-in step). And the imprinting of a cryptographic key is completed at this step A7. Therefore, the 1st write-in step which records the disk ID for encryption on a management domain 11 when the

example in which two sessions of a session 1 (SESSION1) and a session 2 (SESSION2) are written. Moreover, as compared with drawing 8 , as for the flow chart shown in these drawing 9 , drawing 10 , and drawing 11 , it differs in that two kinds of logical format data are written in. In addition, this flow is also performed using the cryptographic key imprinting equipment 19 shown in above-mentioned drawing 7 .

[0105] Moreover, according to the flow chart of drawing 9 , drawing 10 , and drawing 11 , the data layout on CD-R disk 47a (or CD-RW disk 47b) after record was performed becomes like drawing 12 . Drawing 12 is drawing showing the data layout of CD-R [after initialization concerning the 1st operation gestalt of this invention]/RW. The truck 1 on CD-R disk 47a (or CD-RW disk 47b) shown in this drawing 12 is ISO9660. It is logical format data of ** and a truck 2 is logical format data for DirectCD. And a truck 1 is written in, after a truck 2 is written in so that it may mention later.

[0106] First, in step B-2, CD-R disk (CD-R media) 47a is inserted in CD-R / RW drive 46, and, as for the initialization step started from step B1 (refer to drawing 9), the writing of a session 1 is started in step B3. That is, it is Mode Select like what was mentioned above. The memory for commands (not shown) is secured (step B4), it sets in step B5, and a cryptographic key 1 is Select. It is set as the memory for commands, it sets in step B6, and a cryptographic key 2 is Select. It

cryptographic key 2 are set up (the 2nd write-in step, the 3rd write-in step).

[0109] Next, ISO9660 It is ISO9660 to the truck 1 which the writing of logical format data was performed at ** and the attached step (step B16 - step B18), and was secured at the above-mentioned step B8. A logical format is performed. Namely, Write The memory for commands is secured (step B16), and the logical format data for ISO9660 are Write. It is set as the memory for commands (step B17). Furthermore, it sets to step B18 and is Write. A command is published and logical format data are recorded. Therefore, ** and the attached step are performed for ** and the attached step. Moreover, it sets to step B19 and is CloseSession. A command is published, a lead-in groove 1 and lead-out 1 as shown in drawing 12 are written in, and the writing of a session 1 is completed (step B20).

[0110] After this session 1 is completed, in case a session 1 can be read now with usual drive equipment and data are recorded after a session 2, it can encipher using the cryptographic key recorded on the session 1. And B of the topmost part of drawing 11 and the writing of the session 2 which begins from the attached part are started following B shown in drawing 10 , and the attached part.

[0111] Moreover, even if the cryptographic key in a truck 1 is the same as the cryptographic key in a truck 2, they may differ. Thereby, an operator may be able

[0113] Thus, although data with copyrights, such as music and a movie, can copy to the disk of one sheet only once, since it cannot copy to other disks secondarily from the copied disk, there is an advantage from which data with copyright are protected. And it does in this way and there is an advantage which can aim at protection of data with copyright, without adding dues to sound recording / playback device beforehand.

[0114] Furthermore, since the data used as a cryptographic key are distributed and recorded on the existing field, the data distributed and recorded is gathered up and the cryptographic key is generated, even if it does not change the format approach of a disk, there is an advantage which can encipher. moreover, since the distributed approach within a disk can be made to change into versatility if needed, it holds secrecy nature as a cryptographic key, and has the advantage which has the reinforcement raised.

[0115] In addition, since generation of a cryptographic key is made using random-number function Rnd() or Hash Function Hash(), while the same cryptographic key is obtained from the same disk ID etc., the original disk ID etc. is no longer decoded from the outputted cryptographic key. Therefore, secrecy nature increases about a cryptographic key and the secondary copy of data with copyright comes to be prevented.

(A1) The cryptographic key imprinting equipment 19 of the explanation above of

the 1st modification of the 1st operation gestalt is built into other equipments, and the encryption approach of another mode can be performed. Hereafter, those examples are explained as the 3rd modification from the 1st modification of the 1st operation gestalt.

[0116] Drawing 13 is the mimetic diagram of encryption / decryption key recording device concerning the 1st modification of the 1st operation gestalt of this invention. Encryption / decryption recording apparatus 40 shown in this drawing 13 is connected with the internet server 23 through the circuit 36. This encryption / decryption recording apparatus 40 is decryption equipment which decodes that encryption data, offers a personal computer 20, a cable 43, and CD-R / RW drive 22, and is constituted while being encryption equipment which enciphers multimedia data, such as voice, an image, and data, on the initialized CD-R disk or CD-RW disk, and is recorded on it as encryption data.

[0117] Moreover, about the generation method of a cryptographic key, as the 1st operation gestalt explained (refer to drawing 39 - drawing 40), there are three kinds of modes. That is, it may be carried out or encryption may be made to be performed using the information which used Disks ID and MCN or the serial number of ISRC according to the individual, and combined Disks ID and MCN or the serial number of ISRC. Furthermore, encryption can perform information which could use the random-number function which uses Disks ID and MCN or

the serial number of ISRC as a seed, or combined Disks ID and MCN or the serial number of ISRC using the random-number function used as a seed. In addition, encryption can perform information which could use the Hash Function which uses a key message, Disks ID and MCN, or the serial number of ISRC as a seed, or combined a key message, Disks ID and MCN, or the serial number of ISRC using the Hash Function used as a seed.

[0118] Moreover, the disks inserted in CD-R / RW drive 22 are initialized CD-R disk 21a, CD-RW disk 21b or CD-R disk 31a on which data were recorded, and CD-RW disk 31b. Furthermore, the disk ID for encryption is inserted in these management domains 11 (refer to drawing 1) (recorded). In addition, in explanation in each following operation gestalt and its modification, initialized CD-R disk 21a or CD-RW disk 21b may be called the disk for writing. Moreover, CD-R disk 31a or CD-RW disk 31b on which data were recorded may be similarly called the disk for playback. Furthermore, CD-R disk 21a, CD-RW disk 21b, CD-R disk 31a, and CD-RW disk 31b may be summarized, and a disk may be called.

[0119] This personal computer 20 offers decryption means 20c and the 20d of the 2nd cryptographic key generation means, and is constituted. This decryption means 20c decodes the enciphered information using a cryptographic key, multimedia data including the information on voice, an image, data, etc. can be

While offering data area 12b to which it is the field which can read CD-R / RW drive 22, and a user can access the field at arbitration and recording the disk ID for encryption on a management domain 11, the information enciphered by data area 12b is recorded.

[0122] And these functions are demonstrated by the drive equipment in CD-R / RW drive 22 (not shown), respectively. In addition, the detailed explanation about the function of others of CD-R / RW drive 22 is omitted. Furthermore, an internet server 23 enciphers and transmits multimedia data, such as voice, an image, and data, offers encryption media information generation means 23a and cryptographic key generation means 23b, and consists of on the Internet. This encryption media information generation means 23a is the same as that of above-mentioned encryption media information generation means 20a, and omits that detailed explanation. Moreover, cryptographic key generation means 23b can generate a cryptographic key from Disks ID and MCN and the serial number of ISRC.

[0123] Moreover, a circuit 36 is a circuit which connects this internet server 23 and encryption / decryption recording device 40, for example, this circuit function is demonstrated by the Local Area Network. In addition, since the cable 43 is the same as that of what was mentioned above, the explanation is omitted. Thereby, in encryption / decryption recording apparatus 40, the disks ID and MCN of the

inserted disk for writing and the serial number of ISRC are read as a media number in read-out means 22a in CD-R / RW drive 22 (the 1st disk identification information read-out step). After the read media number is inputted into a personal computer 20 through a cable 43, the media number It is transmitted to an internet server 23 through a circuit 36, and sets to cryptographic key generation means 23b in an internet server 23. A cryptographic key is generated in combination with the disks ID and MCN, combination with the serial number of Disks ID and ISRC, or the combination of Disks ID and MCN and the serial number of ISRC (the 1st cryptographic key generation step).

[0124] And in encryption media information generation means 23a in an internet server 23, multimedia data, such as voice, an image, and data, are read (the 1st read-out step), are enciphered by the cryptographic key using the above-mentioned media number, and encryption data are outputted. This encryption data is inputted into CD-R / RW drive 22 in encryption / decryption recording apparatus 40 through a circuit 36. Furthermore, by encryption media information preservation means 22b in CD-R / RW drive 22 Encryption data are generated using the cryptographic key, and a specific disk is generated by being recorded on disc data field 12b (referring to drawing 1) which has the transmitted disk ID (specific record-medium generation step).

[0125] On the other hand, decode is performed as follows. That is, the disk for

writing or the disk for playback is inserted in CD-R / RW drive 22, the disks ID and MCN of the disk and ISRC are read in 2nd read-out means 22c in CD-R / RW drive 22, and these disks ID and MCN and the serial number of ISRC are inputted into a personal computer 20 through a cable 43. Similarly, encryption data are read from the disk for writing, or the disk for playback.

[0126] Moreover, in the 20d of the 2nd cryptographic key generation means in a personal computer 20, a cryptographic key is generated from combination with the disks ID and MCN, combination with the serial number of Disks ID and ISRC, or the combination of Disks ID and MCN and the serial number of ISRC. And in decryption means 20c in a personal computer 20, only when the cryptographic key is in agreement with the transmitted cryptographic key, encryption data are decoded and reproduced and the encryption data of the disk for writing or the disk for playback are decoded using a cryptographic key.

[0127] The encryption and the decryption for the anti-copying of CD-R/RW are performed by such configuration. First, a cryptographic key is inserted in the disk for writing by the initialization step explained with the 1st operation gestalt, and music data are actually recorded after that on the initialized disk for writing. Drawing 14 is the flow chart of the anti-copying approach of of CD-R or CD-RW concerning the 1st modification of the 1st operation gestalt of this invention.

[0128] A user connects first to the site of the Internet the anti-copying step

started from step C1 (step C2), and the media number (Disks ID and MCN, serial number of ISRC) of the disk is transmitted from encryption / decryption recording apparatus 40 to an internet server 23 in step C3. In addition, this step C3 of the condition of data is the usual thing.

[0129] Next, in step C4, an internet server 23 enciphers the transmitted data by the media number (Disks ID and MCN, serial number of ISRC) which is the cryptographic key of a disk (media) proper. Then, in step C5, the encryption data is transmitted from an internet server 23 to encryption / decryption recording device 40. Furthermore, in step C6, the transmitted data is processed by the personal computer 20, and is saved on the disk for writing with it.

[0130] On the other hand, as a decode step, it is step C7, the data is decoded, it is step C8 and the data of the origin of it are reproduced by the cryptographic key of the disk (media) proper, it is step C9 and a decode step is completed. Here, in steps C6, C7, and C8, it cannot decode by any cryptographic keys other than the cryptographic key transmitted at step C3.

[0131] Data cannot be restored, when putting in another way and it is written in disks other than the disk used as a cryptographic key. That is, unless a media number is in agreement, the original data are unreproducible, even if it generates a cryptographic key from the media number and decodes encryption data. Thus, since media numbers (Disks ID and MCN, serial number of ISRC)

required in order to decode the encryption data stored in that specific disk differ even if the specific disk of one sheet with which the cryptographic key was stenciled is obtained and it is going to copy to other disks from this specific disk, the original data are not restored. Furthermore, since a cryptographic key is not transmitted on the direct Internet but Disks ID and MCN and the serial number of ISRC are transmitted, there is no possibility that a cryptographic key may be stolen by others.

[0132] Moreover, although it does in this way and data with copyrights, such as music and a movie, can copy to the disk of one sheet only once, since it cannot copy to other disks secondarily from the copied disk, data with copyright are protected. And it does in this way and there is an advantage which can aim at protection of data with copyright, without adding dues to sound recording / playback device beforehand.

[0133] Furthermore, in the case of record of a cryptographic key, since the data used as a cryptographic key are distributed and recorded on the existing field, the data distributed and recorded can gather up and a cryptographic key is generated, there is an advantage which can encipher without modification of the format approach of a disk. moreover, since the distributed approach within a disk can be changed into versatility if needed, the secrecy nature as a cryptographic key is held and has the advantage to which the reinforcement is raised.

[0134] And since generation of a cryptographic key is made using random-number function Rnd() or Hash Function Hash(), while the same cryptographic key is obtained from the same disk ID etc., the original disk ID etc. is no longer decoded from the outputted cryptographic key. Therefore, secrecy nature increases about a cryptographic key and the secondary copy of data with copyright comes to be prevented.

(A2) A mode which reads data from the explanation music CD of the 2nd modification of the 1st operation gestalt is also possible.

[0135] Drawing 15 is the mimetic diagram of encryption / decryption recording device concerning the 2nd modification of the 1st operation gestalt of this invention. A personal computer 20, and CD-R / RW drive 22 are offered, and also the CD drive 24 and Cables 43a and 43b are offered, and encryption / decryption recording apparatus 40a shown in this drawing 15 is constituted. Moreover, music data enter, the CD media 25 are called the so-called CD for music, and the disk for writing (CD-R disk 21a, CD-RW disk 21b) or the disk for playback (CD-R disk 31a, CD-RW disk 31b) is inserted in CD-R / RW drive 22. Furthermore, the CD drive 24 shown in this drawing 15 reads the CD media 25, is reproduced, and can choose now two or more CD media 25.

[0136] Moreover, data and encryption data can be sent [cable 43a connects a personal computer 20 and the CD drive 24 electrically, and / cable 43b connects

electrically the CD drive 24, and CD-R / RW drive 22, and] now further, and received between a personal computer 20, and CD-R / RW drive 22 by this.

[0137] In addition, a personal computer 20 offers encryption media information generation means 20a, cryptographic key generation means 20b, decryption means 20c, and the 20d of the 2nd cryptographic key generation means, and is constituted. Here, by Disks ID and MCN and the cryptographic key which used the serial number of ISRC, encryption media information generation means 20a enciphers multimedia data, and may output encryption data. Moreover, cryptographic key generation means 20b generates a cryptographic key from Disks ID and MCN and the serial number of ISRC.

[0138] Moreover, about the generation method of a cryptographic key, as the 1st operation gestalt explained (refer to drawing 39 - drawing 40), there are three kinds of modes. That is, it may be carried out or encryption may be made to be performed using the information which used Disks ID and MCN or the serial number of ISRC according to the individual, and combined Disks ID and MCN or the serial number of ISRC. Furthermore, encryption can perform information which could use the random-number function which uses Disks ID and MCN or the serial number of ISRC as a seed, or combined Disks ID and MCN or the serial number of ISRC using the random-number function used as a seed. In addition, encryption can perform information which could use the Hash Function

which uses a key message, Disks ID and MCN, or the serial number of ISRC as a seed, or combined a key message, Disks ID and MCN, or the serial number of ISRC using the Hash Function used as a seed.

[0139] Furthermore, decryption means 20c decodes encryption data using a cryptographic key, multimedia data including the information on voice, an image, data, etc. can be reproduced, and the 20d of the 2nd cryptographic key generation means generates a cryptographic key from Disks ID and MCN and the serial number of ISRC. Since these are the same as that of what was mentioned above, they omit the detailed explanation.

[0140] Moreover, since CD-R / RW drive 22 is the same as that of what was explained in the 1st modification of the 1st operation gestalt, the further explanation is omitted. Thereby, encryption is as follows. That is, in read-out means 22a in CD-R / RW drive 22, the disks ID and MCN of the inserted disk for writing and the serial number of ISRC are read as a media number (the 1st disk identification information read-out step), and the read media number is inputted into a personal computer 20 through Cables 43b and 43a. And a cryptographic key is generated in cryptographic key generation means 20b in a personal computer 20 (the 1st cryptographic key generation step).

[0141] On the other hand, for example, it was recorded on the CD media 25, music data are read in the CD drive 24 (the 1st read-out step), and the data is

inputted into a personal computer 20 through cable 43a. In encryption media information generation means 20a in a personal computer 20, the read data is enciphered using the cryptographic key. And the encryption data Through Cables 43a and 43b, it is inputted into CD-R / RW drive 22, and sets to encryption media information preservation means 22b. Encryption data In case it enciphers, a specific disk is generated by recording on disc data field 12b for writing (referring to drawing 1) which has the read disk ID (specific record-medium generation step).

[0142] Moreover, it is as follows when decoding data. That is, the disk for writing or the disk for playback is inserted in CD-R / RW drive 22. And in 2nd read-out means 22c in CD-R / RW drive 22, the disks ID and MCN and the serial number of ISRC are read, and these are inputted into a personal computer 20 through Cables 43b and 43a. Furthermore, in the 20d of the 2nd cryptographic key generation means in a personal computer 20, a cryptographic key is generated from the read disks ID and MCN and the serial number of ISRC. Moreover, in decryption means 20c in a personal computer 20, the encryption data read from the disk for writing or the disk for playback are decoded only when the cryptographic key is in agreement with the cryptographic key used for encryption, and multimedia data are reproduced.

[0143] The encryption and the decryption for the anti-copying of CD-R/RW are

performed by such configuration. Drawing 16 is the flow chart of the anti-copying approach of of CD-R or CD-RW concerning the 2nd modification of the 1st operation gestalt of this invention. First, in the CD drive 24, after required data are chosen from the CD media 25 (step D2), as for the anti-copying step started from step D1, the data is read (step D3). In addition, this step of the condition of data is the usual thing.

[0144] And in step D4, the data is enciphered by the cryptographic key of the disk (media) proper which combined the serial number of MCN and ISRC, and Disk ID suitably, and the encryption data is saved on the disk for writing (CD-R / RW media) in step D5 by it. On the other hand, as a decode step, it is step D6, the data is decoded, it is step D7 and the decryption data is used by the cryptographic key of the disk (media) proper, it is step D8 and a decode step is completed.

[0145] Moreover, in step D4, after the read data are enciphered, still more nearly another data are read and it can encipher, and in that case, a disk (in drawing 16 , written as CD) is replaced, and the step from step D2 to step D4 is repeated. In addition, in steps D5 and D6, when encryption data are written in disks other than the disk used as a cryptographic key, data cannot be restored.

[0146] Thus, when a user does the 1st copy, multimedia data, such as read voice, an image, and data, are enciphered by the cryptographic key of a disk

proper, and a user can get the specific disk of one sheet. On the contrary, even if a user is going to copy to other disks from the specific disk, since media numbers (Disks ID and MCN, serial number of ISRC) required in order to decode the encryption data stored in the specific disk differ, original music or image data are not restored.

[0147] Moreover, although it does in this way and data with copyrights, such as music and a movie, can copy to the disk of one sheet only once, since it cannot copy to other disks secondarily from the copied disk, data with copyright are protected. And it does in this way and there is an advantage which can aim at protection of data with copyright, without adding dues to sound recording / playback device beforehand.

[0148] Furthermore, in the case of record of a cryptographic key, since the data used as a cryptographic key are distributed and recorded on the existing field, the data distributed and recorded can gather up and a cryptographic key is generated, there is an advantage which can encipher without modification of the format approach of a disk. moreover, since the distributed approach within a disk can be changed into versatility if needed, the secrecy nature as a cryptographic key is held and has the advantage to which the reinforcement is raised.

[0149] And since generation of a cryptographic key is made using random-number function Rnd() or Hash Function Hash(), while the same

cryptographic key is obtained from the same disk ID etc. again, the original disk ID etc. is no longer decoded from the outputted cryptographic key. Therefore, secrecy nature increases about a cryptographic key and the secondary copy of data with copyright comes to be prevented.

(A3) Explanation one side of the 3rd modification of the 1st operation gestalt and the encryption approach of another mode which transmits data can also be performed.

[0150] Drawing 17 is the mimetic diagram of encryption / decryption recording device concerning the 3rd modification of the 1st operation gestalt of this invention. Encryption / decryption recording apparatus 40 shown in this drawing 17 is connected with data forwarding equipment 26 through circuit 36a. This encryption / decryption recording apparatus 40 offers a personal computer 20 and a cable 43, and is constituted. A personal computer 20 offers encryption media information generation means 20a, cryptographic key generation means 20b, decryption means 20c, and the 20d of the 2nd cryptographic key generation means, and is constituted. Since these things are the same as that of what was mentioned above, the detailed explanation is omitted. In addition, since CD-R / RW drive 22, and a cable 43 are the same as that of what was mentioned above, the further explanation is omitted. Moreover, CD-R / RW drive 22 can insert the disk for writing, or the disk for playback.

[0151] Moreover, it is the same as the 1st operation gestalt explained the generation method of a cryptographic key (refer to drawing 39 - drawing 40). That is, it may be carried out or encryption may be made to be performed using the information which used Disks ID and MCN or the serial number of ISRC according to the individual, and combined Disks ID and MCN or the serial number of ISRC.

[0152] Furthermore, encryption can perform information which could use the random-number function which uses Disks ID and MCN or the serial number of ISRC as a seed, or combined Disks ID and MCN or the serial number of ISRC using the random-number function used as a seed. In addition, encryption can perform information which could use the Hash Function which uses a key message, Disks ID and MCN, or the serial number of ISRC as a seed, or combined a key message, Disks ID and MCN, or the serial number of ISRC using the Hash Function used as a seed.

[0153] Moreover, data forwarding equipment 26 sends out a data file etc. to this encryption / decryption recording apparatus 40, carries out A/D conversion of the analog data incorporated, and sends out that digital data. Furthermore, circuit 36a is a circuit which connects data forwarding equipment 26 and encryption / decryption recording device 40, for example, is connected to the serial port (not shown) of a personal computer 20.

[0154] Thereby, in data forwarding equipment 26, A/D conversion of the analog data is carried out, the data is inputted into encryption / decryption recording device 40 through circuit 36a, and it is inputted into a personal computer 20 from the serial port. On the other hand in read-out means 22a in CD-R / RW drive 22, the disks ID and MCN of the inserted disk and the serial number of ISRC are read as a media number, the read media number is inputted into a personal computer 20 through a cable 43, and a cryptographic key is generated in cryptographic key generation means 20b in a personal computer 20.

[0155] And in encryption media information generation means 20a in a personal computer 20, as for the data from a serial port, encryption data are outputted using the cryptographic key, and the encryption data is inputted into CD-R / RW drive 22 through a cable 43. Furthermore, the encryption data is saved by encryption media information preservation means 22b in CD-R / RW drive 22 at disc data field 12b for writing (refer to drawing 1).

[0156] Moreover, it is as follows when decoding from the disk for writing, or the disk for playback. That is, in 2nd read-out means 22c in CD-R / RW drive 22, the disks ID and MCN and the serial number of ISRC are read, and the cryptographic key for decoding is generated in the 20d of the 2nd cryptographic key generation means in a personal computer 20, and the encryption data is decoded in decryption means 20c in a personal computer 20 using the

cryptographic key.

[0157] The encryption and the decryption for the anti-copying of CD-R/RW are performed by such configuration. Drawing 18 is the flow chart of the anti-copying approach of of CD-R or CD-RW concerning the 3rd modification of the 1st operation gestalt of this invention. After the data which save first the encryption step started from step E1 in step E2 are chosen, the file data is incorporated (step E3). In addition, this step of the condition of data is the usual thing.

[0158] And in step E4, the data is enciphered by the cryptographic key of the disk (media) proper which combined the serial number of MCN and ISRC, and Disk ID suitably, and the encryption data is saved on the disk for writing (CD-R / RW media) in step E5 by it. On the other hand, as a decode step, it is step E6, the data is decoded, it is step E7 and the decryption data is used by the cryptographic key of the disk proper, it is step E8 and an encryption step is completed.

[0159] Moreover, in step E2, another data can be read and data are chosen in that case repeatedly. In addition, in steps E5 and E6, when encryption data are written in disks other than the disk used as a cryptographic key, data cannot be restored.

[0160] Thus, when a user does the 1st copy, multimedia data, such as read voice, an image, and data, are enciphered by the cryptographic key of a disk

proper, and a user can get the specific disk of one sheet. On the contrary, even if a user is going to copy to other disks from the specific disk, since media numbers (Disks ID and MCN, serial number of ISRC) required in order to decode the encryption data stored in the specific disk differ, original music or image data are not restored.

[0161] Thus, although data with copyrights, such as music and a movie, can copy to the disk of one sheet only once, since it cannot copy to other disks secondarily from the copied disk, data with copyright are protected. And it does in this way and there is an advantage which can aim at protection of data with copyright, without adding dues to sound recording / playback device beforehand.

[0162] Furthermore, in the case of record of a cryptographic key, since the data used as a cryptographic key are distributed and recorded on the existing field, the data distributed and recorded can gather up and a cryptographic key is generated, there is an advantage which can encipher without modification of the format approach of a disk. moreover, since the distributed approach within a disk can be changed into versatility if needed, the secrecy nature as a cryptographic key is held and has the advantage to which the reinforcement is raised.

[0163] In addition, since generation of a cryptographic key is made using random-number function Rnd() or Hash Function Hash(), while the same cryptographic key is obtained from the same disk ID etc., the original disk ID etc.

is no longer decoded from the outputted cryptographic key. Therefore, secrecy nature increases about a cryptographic key and the secondary copy of data with copyright comes to be prevented.

(B) It can also be used, being able to build into sound equipment the encryption equipment and decryption equipment which were explained in the 1st operation gestalt of the explanation above of the 2nd operation gestalt of this invention.

[0164] Drawing 19 is the mimetic diagram of the sound equipment concerning the 2nd operation gestalt of this invention. The sound equipment 27 shown in this drawing 19 is sound equipment which has an encryption means and a decryption means, offers CD-R / RW drive 42, Loudspeakers 28a and 28b, and the sound re-gray-goods machine 29, and is constituted. Moreover, the disk inserted in this CD-R / RW drive 42 is a disk for playback with which the data other than the initialized disk for writing were recorded. That is, these disks (media) are recorded on optical and the data area 12b (refer to drawing 1) may be written in once [at least] by the user.

[0165] Here, an encryption means (not shown) enciphers multimedia data including the information on voice, data, etc., and can record them as encryption media information, and a decryption means (not shown) can decode the encryption media information which multimedia data including the information on voice, data, etc. were enciphered, and was recorded. Moreover, CD-R / RW

drive 42 enciphers multimedia data including the information on voice, data, etc., can record them as encryption media information, offers read-out means 42a, encryption media information generation means 42b, encryption media information preservation means 42c, the 42d of the 2nd read-out means, 2nd cryptographic key generation means 42e, and 42f of decryption means, and is constituted.

[0166] This read-out means 42a can read the disk ID in the disk for playback with which the disk for writing and data which were initialized were recorded. Moreover, the disk for playback with which this disk for writing and data that were initialized were recorded The management domain 11 where it is the field which can read CD-R / RW drive 42, and a user cannot access the field like the disk 10 shown in drawing 1 , Data area 12b to which it is the field which can read CD-R / RW drive 42, and a user can access the field at arbitration is offered, and the disk ID for encryption is recorded on the management domain 11.

[0167] By Disks ID and MCN and the cryptographic key which used the serial number of ISRC, encryption media information generation means 42b enciphers multimedia data, and may output them as encryption media information, and encryption media information preservation means 42c can save the encryption media information at data area 12b (refer to drawing 1).

[0168] Moreover, it is the same as the 1st operation gestalt explained the

generation method of a cryptographic key (refer to drawing 39 - drawing 40). That is, it may be carried out or encryption may be made to be performed using the information which used Disks ID and MCN or the serial number of ISRC according to the individual, and combined Disks ID and MCN or the serial number of ISRC. Furthermore, encryption can perform information which could use the random-number function which uses Disks ID and MCN or the serial number of ISRC as a seed, or combined Disks ID and MCN or the serial number of ISRC using the random-number function used as a seed. In addition, encryption can perform information which could use the Hash Function which uses a key message, Disks ID and MCN, or the serial number of ISRC as a seed, or combined a key message, Disks ID and MCN, or the serial number of ISRC using the Hash Function used as a seed.

[0169] The 42d of the 2nd read-out means is what can read the disk ID in the disk for writing, and the disk for playback. Furthermore, 2nd cryptographic key generation means 42e It is what generates the cryptographic key for decode from Disks ID and MCN and the serial number of ISRC. 42f of in addition, decryption means The enciphered information is decoded using Disks ID and MCN and the cryptographic key using the serial number of ISRC, and multimedia data including the information on voice, data, etc. can be reproduced.

[0170] Read-out means 42a, encryption media information preservation means

42c, and the 42d of the 2nd read-out means are demonstrated by the drive equipment in CD-R / RW drive 42 among these functions. On the other hand, the function of encryption media information generation means 42b, 2nd cryptographic key generation means 42e, and 42f of decryption means is demonstrated by the software built into the interior.

[0171] Moreover, loudspeaker 28a is a loudspeaker for the left channels of stereo voice, and loudspeaker 28b is a loudspeaker for the right channels of stereo voice. Furthermore, the sound re-gray-goods machine 29 reads music data, is reproduced, amplifies, and may be outputted from Loudspeakers 28a and 28b. Thereby, encryption is as follows. That is, the disks ID and MCN of the disk with which the disk for writing was inserted in read-out means 42a in CD-R / RW drive 42, and the serial number of ISRC are read as a media number. And in encryption media information generation means 42b in CD-R / RW drive 42, multimedia data are enciphered by Disks ID and MCN and the cryptographic key using the serial number of ISRC, and it is outputted as encryption media information. And in encryption media information preservation means 42c in CD-R / RW drive 42, the encryption media information is saved at disc data field 12b for writing (refer to drawing 1).

[0172] Furthermore, about a decryption, it is as follows. That is, in the 42d of the 2nd read-out means in CD-R / RW drive 42, from the disk for writing, or the disk

he specific disk of one sheet. On the contrary, even if a user is going to icryption

other disks from the specific disk, since media numbers (Disks ID and in voice,

rial number of ISRC) required in order to decode the encryption data 43, and

the specific disk differ, the original music data etc. are not restored.

hus, although data with copyrights, such as music, can copy to the disk ned the

neet only once, since it cannot copy to other disks secondarily from the ng 40).

isk, data with copyright are protected. And it does in this way and there ed using

lvantage which can aim at protection of data with copyright, without of ISRC

ues to sound recording / playback device beforehand. ie serial

oreover, since the management domain 11 in a CD-R disk or a CD-RW ch could

data area 12b (refer to drawing 1) are used, the data used as a ne serial

aphic key are distributed and recorded on these fields, the data number

d and recorded can gather up and a cryptographic key is generated in addition,

ryptographic key is recorded, it can encipher, without changing the on which

proach of the existing disk. in addition, since the distributed approach s a seed,

ade to change into versatility if needed, it can raise the reinforcement of ISRC

tographic key.

addition, a mode which performs only playback is also possible. l by the

20 is the mimetic diagram of other sound equipments concerning the , CD-R /

ation gestalt of this invention. Sound equipment 27a shown in this se disks

(media) and recorded on them, such as voice and data, using the cryptographic key of the CD-R disks 21a and 31a or the CD-RW disks 21b and 31b, offers the 42d of the 2nd read-out means, 2nd cryptographic key generation means 42e, and 42f of decryption means, and is constituted. In addition, Loudspeakers 28a and 28b are the same as that of what was mentioned above.

[0181] By such configuration, while musical playback is performed, decode is performed. That is, in the 42d of the 2nd read-out means in CD-R / RW drive 43, the disks ID and MCN of the disk for playback and the serial number of ISRC are read, in 2nd cryptographic key generation means 42e, a cryptographic key is generated, and the encryption data of the disk for playback are decoded in 42f of decryption means using the cryptographic key, and multimedia data, such as voice and data, are reproduced.

[0182] Here, only the information by which the original music data are not restored and the data which were enciphered by disks other than this disk and recorded on them were recorded only on the disk of one sheet since the cryptographic keys of a disk proper differed is reproduced. Thus, since a user is reincarnated by decoding by the cryptographic key of a disk proper, he cannot restore the original music data etc. in any cryptographic keys other than the cryptographic key.

[0183] Thus, although data with copyrights, such as music, can copy to the disk

of one sheet only once, since it cannot copy to other disks secondarily from the copied disk, data with copyright are protected. And it does in this way and there is an advantage which can aim at protection of data with copyright, without adding dues to sound recording / playback device beforehand.

[0184] Furthermore, in the case of record of a cryptographic key, since the data used as a cryptographic key are distributed and recorded on the existing field, the data distributed and recorded can gather up and a cryptographic key is generated, there is an advantage which can encipher without modification of the format approach of a disk. moreover, since the distributed approach within a disk can be changed into versatility if needed, the secrecy nature as a cryptographic key is held and has the advantage to which the reinforcement is raised.

[0185] In addition, since generation of a cryptographic key is made using random-number function Rnd() or Hash Function Hash(), while the same cryptographic key is obtained from the same disk ID etc., the original disk ID etc. is no longer decoded from the outputted cryptographic key. Therefore, secrecy nature increases about a cryptographic key and the secondary copy of data with copyright comes to be prevented.

(B1) It can also be used, being able to include the function which was explained in the 2nd operation gestalt of explanation of the 1st modification of the 2nd operation gestalt of this invention and which can be enciphered and decoded in

media number.

[0190] On the other hand, in AV equipment 34, the data of voice or an image are reproduced, the data of this reproduced voice and image are inputted into this CD-R / television 33 with RW drive through cable 43d, playback and magnification are carried out suitably and that data is outputted from the loudspeakers 28a and 28b on either side through Cables 43b and 43c.

[0191] Moreover, on the other hand, in encryption media information generation means 42b in this CD-R / television 33 with RW drive, the cryptographic key of a disk proper is created by Disks ID and MCN and the serial number of ISRC, and, as for data, such as that music, encryption data are outputted using that cryptographic key. And the encryption data is saved by encryption media information preservation means 42c in CD-R / television 33 with RW drive at disc data field 12b for writing.

[0192] Furthermore, about a decryption, it is as follows. Namely, it sets for the 42d of the 2nd read-out means in CD-R / television 33 with RW drive. Disks ID and MCN and the serial number of ISRC are read, and it sets to 2nd cryptographic key generation means 42e. From Disks ID and MCN and the serial number of ISRC, a cryptographic key is generated, and the encryption data is further decoded by the cryptographic key in 42f of decryption means, and multimedia data, such as voice, an image, and data, are reproduced.

[0193] By such configuration, a user performs the voice data and the image copy of data for illegal copy prevention of CD-R/RW which were enciphered while reproducing the information on the music stored in this sound, image, and data station 32, or an image. That is, when a user does the 1st copy, first, the information on voice or an image is read and the information on the read voice and image is enciphered by the cryptographic key of a disk proper. Therefore, a user can get the specific disk of one sheet.

[0194] On the contrary, even if a user is going to copy to other disks from the specific disk, since media numbers (Disks ID and MCN, serial number of ISRC) required in order to decode the encryption data stored in the specific disk differ, original music or image data are not restored. Thus, since it is recorded only on the disk of one sheet, being illegally copied of work data is lost.

[0195] In addition, by performing encryption using random-number function Rnd() or Hash Function Hash(), the same cryptographic key comes to be obtained from the same disk ID etc., and decode of the original disk ID etc. becomes impossible and secrecy nature increases.

(B-2) Only explanation one side of the 2nd modification of the 2nd operation gestalt of this invention, and in playback, it is as follows.

[0196] Drawing 22 is the mimetic diagram of the sound, image, and data station concerning the 2nd modification of the 2nd operation gestalt of this invention.

The encryption media information that multimedia data including the information on voice, an image, data, etc. were enciphered and recorded is decoded, and it can reproduce, and the sound, the image, and data station 32a shown in this drawing 22 offer CD-R / television 33 with RW drive, and Loudspeakers 28a and 28b, and is constituted.

[0197] This CD-R / television 33 with RW drive decode multimedia data, such as voice which is enciphered by these disks and recorded on them, an image, and data, using the cryptographic key of a CD-R disk or a CD-RW disk, offers the 42d of the 2nd read-out means, 2nd cryptographic key generation means 42e, and 42f of decryption means, and is constituted. Since these are the same as that of what was mentioned above, they omit the further explanation.

[0198] Moreover, it is the same as the 1st operation gestalt explained the generation method of encryption (refer to drawing 39 - drawing 40). That is, it may be carried out or encryption may be made to be performed using the information which used Disks ID and MCN or the serial number of ISRC according to the individual, and combined Disks ID and MCN or the serial number of ISRC. Furthermore, encryption can perform information which could use the random-number function which uses Disks ID and MCN or the serial number of ISRC as a seed, or combined Disks ID and MCN or the serial number of ISRC using the random-number function used as a seed. In addition,

encryption can perform information which could use the Hash Function which uses a key message, Disks ID and MCN, or the serial number of ISRC as a seed, or combined a key message, Disks ID and MCN, or the serial number of ISRC using the Hash Function used as a seed.

[0199] Moreover, the disk inserted is a disk for playback which was generated by the cryptographic key and with which encryption data are recorded. Thereby, in the 42d of the 2nd read-out means in CD-R / television 33 with RW drive, the disks ID and MCN of the disk for playback and the serial number of ISRC are read, and a cryptographic key is generated in 2nd cryptographic key generation means 42e. And in 42f of decryption means, the encryption data of the disk for playback are decoded using the cryptographic key.

[0200] As for CD-R / television 33 with RW drive, the anti-copying of the disk for playback is made by such configuration. That is, only the information by which original music or image data are not restored and the data which were enciphered by disks other than this disk and recorded on them were recorded only on the disk of one sheet since the cryptographic keys of a disk proper differed is reproduced.

[0201] Thus, since the data with copyrights, such as music and a movie, cannot be secondarily copied to other disks from the disk of one sheet, data with copyright are protected. And it does in this way and there is an advantage which

can aim at protection of data with copyright, without adding dues to sound recording / playback device beforehand. Furthermore, in the case of record of a cryptographic key, since the data used as a cryptographic key are distributed and recorded on the existing field, the data distributed and recorded can gather up and a cryptographic key is generated, there is an advantage which can encipher without modification of the format approach of a disk. moreover, since the distributed approach within a disk can be changed into versatility if needed, the secrecy nature as a cryptographic key is held and has the advantage to which the reinforcement is raised.

[0202] In addition, since encryption is performed using random-number function Rnd() or Hash Function Hash(), the same cryptographic key is obtained from the same disk ID etc. Moreover, since decode of the original disk ID etc. becomes impossible, secrecy nature increases.

(C) Explain further the application of explanation and others of the 3rd operation gestalt of this invention.

[0203] Drawing 23 is drawing showing encryption / decryption recording device concerning the 3rd operation gestalt of this invention. Encryption / decryption recording apparatus 40b shown in this drawing 23 decodes the encryption data which enciphered the digital data, and carried out record on a CD-R disk or a CD-RW disk using the cryptographic key of a CD-R disk or a CD-RW disk, and

were recorded on the CD-R disk or the CD-RW disk, and takes out that decryption data. And this encryption / decryption recording apparatus 40b offers the circumference store 35, a personal computer 20, and CD-R / RW drive 22, and is constituted. Moreover, this encryption / decryption recording device 40b can change the encryption approach into arbitration as an addition function.

[0204] This circumference store 35 stores data, and the data stored in this are used for selection of the encryption approach like a hard disk or an MO drive. Selection of this encryption approach means choosing it as arbitration from DES, RC4, IDEA, etc. Moreover, a personal computer 20, and CD-R / RW drive 22 are the same as that of what was explained in the 1st modification of the 1st operation gestalt mentioned above. Furthermore, the disk inserted is an initialized disk. Moreover, Cables 43a and 43b connect between these devices.

[0205] In addition, since CD-R / RW drive 22, and Cables 43a and 43b are the same as that of what was mentioned above, the further explanation is omitted. This sets to read-out means 22a in CD-R / RW drive 22. The disks ID and MCN of the inserted disk and the serial number of ISRC are read as a media number. The read media number Through cable 43b, it is inputted into a personal computer 20 and a cryptographic key is generated in cryptographic key generation means 20b in a personal computer 20 by the encryption approach based on the data incorporated from the circumference store 35.

[0206] Moreover, it is the same as the 1st operation gestalt explained the generation method of a cryptographic key (refer to drawing 39 - drawing 40). That is, it may be carried out or encryption may be made to be performed using the information which used Disks ID and MCN or the serial number of ISRC according to the individual, and combined Disks ID and MCN or the serial number of ISRC. Furthermore, encryption can perform information which could use the random-number function which uses Disks ID and MCN or the serial number of ISRC as a seed, or combined Disks ID and MCN or the serial number of ISRC using the random-number function used as a seed. In addition, encryption can perform information which could use the Hash Function which uses a key message, Disks ID and MCN, or the serial number of ISRC as a seed, or combined a key message, Disks ID and MCN, or the serial number of ISRC using the Hash Function used as a seed.

[0207] And in encryption media information generation means 20a in a personal computer 20, the encryption data enciphered by that cryptographic key are outputted, and this encryption data is saved by encryption media information preservation means 22b in CD-R / RW drive 22 at disc data field 12b for writing (refer to drawing 1). Here, the user who operates this encryption / decryption recording device 40b incorporates the data for making it another code in a personal computer 20 through cable 43a from the circumference store 35, when

changing the encryption approach. And a cryptographic key can be changed now by making it the another encryption approach.

[0208] Furthermore, it is as follows when decoding from the disk for writing, or the disk for playback. That is, in 2nd read-out means 22c in CD-R / RW drive 22, the disks ID and MCN and the serial number of ISRC are read, and the encryption data of the disk for writing or the disk for playback are decoded in decryption means 20c in a personal computer 20 using a cryptographic key.

[0209] By such configuration, a user copies the digital data with which it was enciphered for illegal copy prevention of CD-R/RW using it while being able to use the program for changing the encryption approach stored in this encryption / decryption recording device 40b etc. That is, in order to change the encryption approach into RC4 from DES, from the circumference storage 35, a user incorporates the program for the encryption etc. and changes the encryption approach. Moreover, this change can be made freely.

[0210] And like what was mentioned above, when carrying out the 1st copy, first, a user reads digital data and enciphers the read digital data by the cryptographic key of a disk proper. Therefore, a user can get the specific disk of one sheet. On the contrary, even if a user is going to copy to other disks from the specific disk, since media numbers (Disks ID and MCN, serial number of ISRC) required in order to decode the encryption data stored in the specific disk differ, the original

digital data is not restored.

[0211] thus, since the encryption approach can change into versatility if needed, the secrecy nature as a code is held and there is an advantage which can raise the reinforcement. Moreover, it does in this way, and although the digital data which included with [, such as music and a movie] copyright can copy to the disk of one sheet only once, since it cannot copy to other disks secondarily from the copied disk, data with copyright are protected. And it does in this way and there is an advantage which can aim at protection of data with copyright, without adding dues to sound recording / playback device beforehand.

[0212] Furthermore, in the case of record of a cryptographic key, since the data used as a cryptographic key are distributed and recorded on the existing field, the data distributed and recorded can gather up and a cryptographic key is generated, there is an advantage which can encipher without modification of the format approach of a disk. moreover, since the distributed approach within a disk can be changed into versatility if needed, the secrecy nature as a cryptographic key is held and has the advantage to which the reinforcement is raised.

[0213] In addition, since encryption is performed using random-number function Rnd() or Hash Function Hash(), the same cryptographic key is obtained from the same disk ID etc. Moreover, since decode of the original disk ID etc. becomes impossible, secrecy nature increases.

(D) In addition, this invention is not limited to the embodiment mentioned above and its modification, it is the range which does not deviate from the meaning of this invention, and can deform variously and can be carried out.

[0214] First, other modes can also perform the method of combination of the cryptographic key by the difference in the die length of a cryptographic key mentioned above. Since reading of Disk ID may be impossible depending on hardware, it can also use two kinds such as MCN and the serial number of ISRC collectively, and simple encryption comes to be able to do it in that case.

[0215] In addition, it is a difficult point that the rationale of safety is not established but the demerit of MD method moreover introduces parallel processing. And when using a 128-bit hash algorithm (MD5), in order to reduce the probability which generates the same message digest, what combined the original disk ID etc. is preferably taken as bit length 128 bits or more.

[0216] Moreover, a secondary manufacturer and those who it not only means a consuming public etc., but use it for records of the initialized disk, such as data, also include the word of the user who used it by this invention. Furthermore, the circuit 36 explained in the 1st modification of the 1st operation gestalt contains not only a Local Area Network but a circuit like the so-called dialup connection which used the telephone line. And even if the part where the cryptographic key for encryption is generated is not an internet server 23, also with a personal

computer 20, it is possible and transmits only a cryptographic key to an internet server 23 in that case. In addition, in this case, applying is also possible so that the information between the data forwarding machine in online karaoke and an accepting station may be exchanged.

[0217] And circuit 36a not only of a serial port but using other ports which connects the data forwarding equipment 26 explained in the 2nd modification of the 1st operation gestalt and a personal computer 20 is possible, and can transmit data further using wireless. In addition, in the 1st modification, as AV equipment 34, it may be not only a video regenerative apparatus but satellite broadcasting service, and a terrestrial electric-wave receiving set, and you may be domestic terminals, such as CATV, at the 2nd operation gestalt.

[0218] In addition, in drawing 8 , and 9 and 10, what is displayed as the channel means a channel and these are the same semantics. Furthermore, what is displayed as PC by drawing 14 means a personal computer 20. Moreover, in drawing 14 , and 16 and 18, what is displayed as the code key means the cryptographic key. In addition, drawing 24 and phi currently displayed on 25 and 26 are the notations showing the die length of the diameter of a millimeter unit.

[0219] Moreover, in the above explanation, although CD-R/RW was made into the example, this invention can be applied to other media, without limiting to CD-R/RW. For example, also in media, such as DVD-R, DVD-RAM, and

DVD-RW, disk information is recordable on a management domain. In addition, as long as it is a two-layer mold medium and a double-sided mold medium, a management domain may be established only in one layer or the whole surface inside, and may be established in each class or each field.

[0220]

[Effect of the Invention] The management domain where according to the record medium of this invention it is the field which a reader can read and a user cannot access the field as explained in full detail above, Since the data area where it is the field which a reader can read and a user can access the field at arbitration is offered and the disk identification information for encryption is recorded on the management domain, although only one sheet can obtain a specific disk, a user Even if a user is going to copy to other disks from the specific disk Since media numbers (Disks ID and MCN, serial number of ISRC) required in order to decode the encryption data stored in the specific disk differ Since original music or image data are not restored and it cannot copy to other disks secondarily from the copied disk, there is an advantage from which data with copyright are protected. Furthermore, there is an advantage which can aim at protection of data with copyright, without adding dues to sound recording / playback device beforehand. in addition, since there is an advantage which can encipher without changing the existing format approach of a disk and the distributed approach of

a cryptographic key can be changed into versatility if needed, the secrecy nature as a cryptographic key is held and there is an advantage which can raise the reinforcement (claim 1).

[0221] In addition, according to this invention, there is the effectiveness thru/or the advantage like ** - ** shown below.

** This invention is the point that the disk identification information for encryption is recorded on a disk, and unlike the technique of well-known reference 1 publication in which particular part record of the medium is carried out for the specific value for anti-copying therefore, this invention can encipher now mere not anti-copying but data, and has the advantage that the dependability of data protection becomes very high by this.

[0222] ** This invention has the advantage as which the key information on encryption can encipher it unlike the technique of the well-known reference 2 publication recorded on a non-data storage area by a bar code and the geometrical pattern therefore in that the disk identification information for encryption is recorded on "the management domain where it is the field which a reader can read and a user cannot access the field" according to this invention without using the key information reading means of dedication.

[0223] ** In a recordable disk, different disk identification information for every disk this invention at the point recorded on "the management domain where it is

the field which a reader can read and a user cannot access the field" Unlike the technique of the well-known reference 3 publication recorded on two record sections where a record format differs from a recording layer, respectively therefore, according to this invention, encryption data and cryptographic key information A cryptographic key can be set up according to a disk individual, there is an advantage to which the dependability of data protection becomes very high, and there is an advantage which can encipher without using the key information reading means of dedication.

[0224] ** The field which should record the disk identification information for encryption this invention at the point concretely made into "the management domain where it is the field which a reader can read and a user cannot access the field" If a user is going to rewrite [a TOC field], the advantage to which the possibility of an alteration of the data encryption key by the user can make [unlike the technique of the well-known reference 4 publication which enables rewriting/elimination therefore] information on the field very low according to this invention is in arbitration.

[0225] Moreover, while media information, such as voice, an image, and data, is recorded on the data area at least as encryption media information enciphered by the cryptographic key which used the above-mentioned disk identification information and was generated If the medium identification number information

which a user can read can also constitute so that it may be distributed and recorded, and it makes it such Since media numbers (Disks ID and MCN, serial number of ISRC) required in order to decode the encryption data stored in the specific disk differ even if it is going to copy to other disks Since original music or image data are not restored and it cannot copy to other disks secondarily from the copied disk, there is an advantage from which data with copyright are protected (claim 2).

[0226] Furthermore, the management domain where according to the initialization approach of the record medium of this invention it is the field which a reader can read and a user cannot access the field, It is the field which a reader can read and is the initialization approach of a record medium that the user offered the data area which can access the field at arbitration. The 1st write-in step which is constituted so that the disk identification information for encryption may be recorded on a management domain, and records the disk identification information for encryption on a management domain, The 2nd write-in step which records medium identification number information on a data area by the mode dimorphism formula of a Q channel sub-code, If it may be offered and constituted by the data area and the 3rd write-in step which records serial number information is carried out in this way in mode 3 format of a Q channel sub-code in it Too, it cannot copy to other disks secondarily from the copied disk,

but there is an advantage from which data with copyright are protected. in addition, since there is an advantage which can encipher without changing the existing format approach of a disk and the distributed approach of a cryptographic key can be changed into versatility if needed, the secrecy nature as a cryptographic key is held and there is an advantage which can raise the reinforcement (claims 5 and 6).

[0227] And after performing initialization which records the disk identification information for encryption on a management domain according to the encryption approach on the record medium of this invention By enciphering by the cryptographic key using the above-mentioned disk identification information at least, and recording media information including voice, an image, and any one information on the data on a data area as encryption media information Although data with copyrights, such as music and a movie, can copy to the disk of one sheet only once since the encryption step which generates a specific record medium is offered and it is constituted Since it cannot copy to other disks secondarily from the copied disk, there is an advantage from which data with copyright are protected. And there is an advantage which can aim at protection of data with copyright, without adding dues to sound recording / playback device beforehand (claim 7).

[0228] Moreover, the 1st write-in step at which the initialization records the disk

identification information for encryption on a management domain, The 2nd write-in step which records medium identification number information on a data area by the mode dimorphism formula of a Q channel sub-code, It consists of 3rd write-in steps which record serial number information on a data area in mode 3 format of a Q channel sub-code. The 1st disk identification information read-out step from which the encryption step reads disk identification information as the 1st disk identification information, The 1st cryptographic key generation step which generates the 1st cryptographic key combining the 1st disk identification information and at least one information in medium identification number information and serial number information, The 1st read-out step which reads media information from an external device, and by generating encryption media information using the 1st cryptographic key, and recording on the data area which has the 1st disk identification information If it may be offered and constituted and the specific record-medium generation step which generates a specific record medium is carried out in this way, it cannot copy to other disks secondarily from the copied disk, but there is an advantage from which data with copyright are protected (claims 8 and 9).

[0229] In addition, according to the encryption equipment of this invention, the initialized record medium sets for a read-out means. Disk identification information is read at least and it sets for an encryption media information

generation means. Media information, such as voice, an image, and data, is enciphered at least by the cryptographic key using the above-mentioned disk identification information in a data area, and it sets for an encryption media information preservation means. Since encryption media information is constituted so that it may be saved in the data area of the record medium which has the same disk identification information Too, it cannot copy to other disks secondarily from the copied disk, but there is an advantage from which data with copyright are protected (claim 10).

[0230] Moreover, according to the decryption equipment of this invention, the record medium with which the enciphered information was recorded sets for the 2nd read-out means. Disk identification information is read at least and it sets for the 2nd cryptographic key generation means. Since it is constituted so that the 2nd cryptographic key may be generated, the enciphered information may be decoded in a decryption means using the 2nd cryptographic key from disk identification information at least and media information, such as voice, an image, and data, may be reproduced since there is an advantage which can encipher without changing the existing format approach of a disk and the distributed approach of a cryptographic key can be changed into versatility if needed, the secrecy nature as a cryptographic key is held and there is an advantage which can raise the reinforcement (claim 11).

[0231] Furthermore, while according to the sound, image, and the data station of this invention enciphering media information, such as voice, an image, and data, to the initialized record medium and being able to record on it as encryption media information Since the record medium with which the enciphered information was recorded is decoded using the 2nd cryptographic key generated from disk identification information at least and media information, such as voice, an image, and data, is reproduced Since it cannot copy to other disks secondarily from the copied disk, there is an advantage from which data with copyright are protected. moreover, since there is an advantage which can encipher without changing the existing format approach of a disk and the distributed approach of a cryptographic key can be changed into versatility if needed, the secrecy nature as a cryptographic key is held and there is an advantage which can raise the reinforcement (claims 12 and 13).

[0232] Moreover, if the above-mentioned record medium may be recorded on optical, a data area may be written in once [at least] by the user and it does [therefore] in this way, since it cannot copy to other disks secondarily from the copied disk, there is an advantage from which data with copyright are protected (claims 3 and 4). In addition, the above-mentioned encryption may be made to be performed using disk identification information and the information which combined serial number information or these with the medium identification

number information list. Moreover, it may be made to be carried out using the random-number function which uses as a seed disk identification information and information which combined serial number information or these with the medium identification number information list. Furthermore, if it may be made to be carried out using the Hash Function used as a seed and a key message, disk identification information, and information that combined serial number information or these with the medium identification number information list are carried out in this way Since the original disk identification information etc. is not restored, the secrecy nature of media information increases and data with copyright come (claim 14 - claim 20) to be protected.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing showing arrangement with the non-data area of CD-R/RW where this invention is applied, and a data area.

[Drawing 2] (a) is drawing showing notional field arrangement of CD-R/initialized RW, and (b) is drawing showing notional field arrangement of CD-R/RW on which encryption data were recorded.

[Drawing 3] It is drawing for explaining being enciphered by the media number.

[Drawing 4] It is drawing for explaining being decrypted by the media number.

[Drawing 5] It is drawing for explaining that a secondary copy is not made.

[Drawing 6] It is drawing showing the encryption approach using a cryptographic key.

[Drawing 7] It is the mimetic diagram of the cryptographic key imprinting equipment concerning the 1st operation gestalt of this invention.

[Drawing 8] It is an initialization flow chart in the anti-copying approach of CD-RW concerning the 1st operation gestalt of this invention.

[Drawing 9] It is an initialization flow chart in the anti-copying approach of CD-R concerning the 1st operation gestalt of this invention.

[Drawing 10] It is an initialization flow chart in the anti-copying approach of CD-R concerning the 1st operation gestalt of this invention.

[Drawing 11] It is an initialization flow chart in the anti-copying approach of CD-R concerning the 1st operation gestalt of this invention.

[Drawing 12] It is drawing showing the data layout of CD-R [after initialization concerning the 1st operation gestalt of this invention]/RW.

[Drawing 13] It is the mimetic diagram of encryption / decryption key recording device concerning the 1st modification of the 1st operation gestalt of this invention.

[Drawing 14] It is the flow chart of the anti-copying approach of of CD-R or CD-RW concerning the 1st modification of the 1st operation gestalt of this invention.

[Drawing 15] It is the mimetic diagram of encryption / decryption recording device concerning the 2nd modification of the 1st operation gestalt of this invention.

[Drawing 16] It is the flow chart of the anti-copying approach of of CD-R or CD-RW concerning the 2nd modification of the 1st operation gestalt of this invention.

[Drawing 17] It is the mimetic diagram of encryption / decryption recording device concerning the 3rd modification of the 1st operation gestalt of this invention.

[Drawing 18] It is the flow chart of the anti-copying approach of of CD-R or CD-RW concerning the modification of the 1st operation gestalt of this invention.

[Drawing 19] It is the mimetic diagram of the sound equipment concerning the 2nd operation gestalt of this invention.

[Drawing 20] It is the mimetic diagram of other sound equipments concerning the 2nd operation gestalt of this invention.

[Drawing 21] It is the mimetic diagram of the sound, image, and data station concerning the 1st modification of the 2nd operation gestalt of this invention.

[Drawing 22] It is the mimetic diagram of the sound, image, and data station concerning the 2nd modification of the 2nd operation gestalt of this invention.

[Drawing 23] It is the mimetic diagram of encryption / decryption equipment concerning the 3rd operation gestalt of this invention.

[Drawing 24] It is drawing showing arrangement with the non-data area of CD-R/RW, and a data area.

[Drawing 25] It is drawing showing the disc data structure in the middle of write-in.

[Drawing 26] It is drawing showing the disc data structure after write-in termination.

[Drawing 27] It is drawing showing a format of a subcoding frame.

[Drawing 28] It is drawing showing a detailed format of a frame.

[Drawing 29] It is drawing having shown the sub coding region in the detail.

[Drawing 30] It is drawing showing the frame structure in the mode 1 of Q channels.

[Drawing 31] It is drawing showing the frame structure in the mode 2 of Q channels.

[Drawing 32] It is drawing showing the data format at the time of drive equipment recording MCN.

[Drawing 33] It is drawing showing a format of the MCN data which drive

equipment read.

[Drawing 34] It is drawing showing the frame structure in the mode 3 of Q channels.

[Drawing 35] It is drawing showing a format of the ISRC data which drive equipment read.

[Drawing 36] It is drawing showing the 1st example of data logging.

[Drawing 37] It is drawing showing the 2nd example of data logging.

[Drawing 38] It is drawing showing the 3rd example of data logging.

[Drawing 39] (a) - (c) is the explanatory view of the cryptographic key generation method which used three kinds of cryptographic keys, respectively.

[Drawing 40] It is drawing showing the example program of a Hash Function.

[Description of Notations]

1 1' Media number (media number field)

10, 10', 60 Disk (media)

11 61 Management domain

12 62 User area

12a, 62a Lead-in groove field

12b, 54a, 62b Data area

12c, 62c Lead-out field

19 Cryptographic Key Imprinting Equipment

20 Personal Computer

20a, 23a, 42b Encryption media information generation means

20b, 23b Cryptographic key generation means

20c, 42f Decryption means

20d, 42e The 2nd cryptographic key generation means

21a, 31a, 47a CD-R disk (CD-R media)

21b, 31b, 47b CD-RW disk (CD-RW media)

22, 42, 46 CD-R / RW drive

22a, 42a Read-out means

22b, 42c Encryption media information preservation means

23 Internet Server

24 CD Drive

26 Data Forwarding Equipment

27 27a Sound equipment

28a, 28b Loudspeaker

29 Sound Re-Gray-Goods Machine

33 CD-R / Television with RW Drive

32 Sound, Image, and Data Station

33a, 33b, 33c, 43, 43a, 43b Cable

34 AV Equipment

35 Circumference Storage

36 36a Circuit

40, 40a, 40b Encryption / decryption recording device

22c, 42d The 2nd read-out means

45 Media Number Setting Means

53 Block

53a Frame

54 Sub Coding Region

54b Field

55 Frame in Mode 1

56 Frame in Mode 2

57 Frame in Mode 3

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－202694
（P2001－202694A）
(43)公開日　平成13年７月27日(2001.7.27)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｄ０４４
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｄ	５Ｄ１１０
Ｇ１１Ｂ　20/12		Ｇ１１Ｂ　20/12		５Ｊ１０４
27/00		27/00	Ａ	

審査請求　未請求　請求項の数20　ＯＬ　（全 42 頁）　最終頁に続く

(21)出願番号　特願2000－170599(P2000－170599)

(22)出願日　平成12年６月７日(2000.6.7)

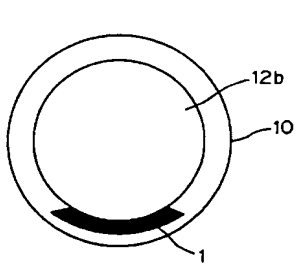
(31)優先権主張番号　特願平11－177470
(32)優先日　平成11年６月23日(1999.6.23)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平11－319514
(32)優先日　平成11年11月10日(1999.11.10)
(33)優先権主張国　日本（ＪＰ）

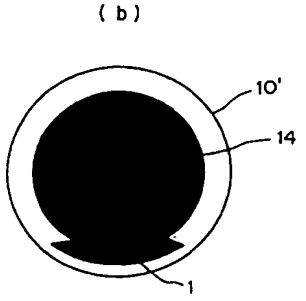
(71)出願人　000005968
三菱化学株式会社
東京都千代田区丸の内二丁目５番２号
(72)発明者　金山　正明
神奈川県横浜市青葉区鴨志田町1000番地
三菱化学株式会社横浜総合研究所内
(72)発明者　藤原　毅
神奈川県横浜市青葉区鴨志田町1000番地
三菱化学株式会社横浜総合研究所内
(74)代理人　100092978
弁理士　真田　有

最終頁に続く

(54)【発明の名称】　記録媒体、記録媒体の初期化方法並びに記録媒体上での暗号化方法及び暗号化装置並びに復号化装置並びに音響・映像・データ装置

(57)【要約】
【課題】　ＣＤ－Ｒディスク又はＣＤ－ＲＷディスクにおいて、既存のフォーマット方法を利用してディスクに所定の初期化を施すことにより、ユーザが音楽，映画，コンピュータプログラムデータ等の著作権付きデータを、１枚のディスクに１回だけコピーできるが、そのコピーされたディスクから他のディスクへ二次コピーはできないようにして、著作権付きデータの保護が図れるようにする。
【解決手段】　ＣＤ－Ｒディスク（又はＣＤ－ＲＷディスク）１０において、１０進数の６桁のディスクＩＤ，１０進数１３桁のＭＣＮ，１０進数５桁ＩＳＲＣシリアル番号を組み合わせた暗号化キーであるメディア番号１と、このメディア番号１によって暗号化された暗号化データ１４とが記録された、特定ディスク１０′として生成されるようにする。





1

【特許請求の範囲】

【請求項１】　読み取り装置が読み出し可能な領域であってユーザはその領域をアクセスできない管理領域と、該読み取り装置が読み出し可能な領域であってユーザがその領域を任意にアクセスできるデータ領域とをそなえ、

該管理領域に、暗号化のためのディスク識別情報が記録されていることを特徴とする、記録媒体。

【請求項２】　該データ領域に、音声、映像、データのいずれか一つの情報を含むメディア情報が、少なくとも該ディスク識別情報を用いて生成された暗号鍵によって暗号化された暗号化メディア情報として記録されるとともに、ユーザが読み出しうる媒体識別番号情報が、分散されて記録されたことを特徴とする、請求項１に記載の記録媒体。

【請求項３】　該記録媒体が、光学式に記録されることを特徴とする、請求項１又は請求項２に記載の記録媒体。

【請求項４】　該データ領域が、ユーザによって少なくとも１回は書き込まれ得ることを特徴とする、請求項１～請求項３のいずれか一項に記載の記録媒体。

【請求項５】　読み取り装置が読み出し可能な領域であってユーザはその領域をアクセスできない管理領域と、該読み取り装置が読み出し可能な領域であってユーザがその領域を任意にアクセスできるデータ領域とをそなえた記録媒体の初期化方法であって、

該管理領域に暗号化のためのディスク識別情報を記録することを特徴とする、記録媒体の初期化方法。

【請求項６】　該ディスク識別情報を記録するに当たり、

該管理領域に暗号化のためのディスク識別情報を記録する第１書込ステップと、該データ領域にＱチャネルサブコードのモード２形式で媒体識別番号情報を記録する第２書込ステップと、

該データ領域にＱチャネルサブコードのモード３形式でシリアル番号情報を記録する第３書込ステップとをそなえて構成されたことを特徴とする、請求項５に記載の記録媒体の初期化方法。

【請求項７】　読み取り装置が読み出し可能な領域であってユーザはその領域をアクセスできない管理領域と、該読み取り装置が読み出し可能な領域であってユーザがその領域を任意にアクセスできるデータ領域をそなえた記録媒体上での暗号化方法であって、

該管理領域に暗号化のためのディスク識別情報を記録する初期化を行なった後に、

音声、映像、データのいずれか一つの情報を含むメディア情報を、少なくとも上記のディスク識別情報を用いた暗号鍵によって暗号化し、暗号化メディア情報として該データ領域に記録することにより、特定記録媒体を生成する暗号化ステップをそなえて構成されたことを特徴とする、記録媒体上での暗号化方法。

2

【請求項８】　該初期化が、該管理領域に暗号化のためのディスク識別情報を記録する第１書込ステップと、該データ領域にＱチャネルサブコードのモード２形式で媒体識別番号情報を記録する第２書込ステップと、該データ領域にＱチャネルサブコードのモード３形式でシリアル番号情報を記録する第３書込ステップとから構成されたことを特徴とする、請求項７に記載の記録媒体上での暗号化方法。

【請求項９】　該暗号化ステップが、

該ディスク識別情報を第１ディスク識別情報として読み出す第１ディスク識別情報読出ステップと、

該第１ディスク識別情報と、該媒体識別番号情報及び該シリアル番号情報のうちの少なくとも一つの情報とを組み合わせて該第１暗号鍵を生成する第１暗号鍵生成ステップと、

外部装置より該メディア情報を読み出す第１読出ステップと、

該第１暗号鍵を用いて該暗号化メディア情報を生成し、該第１ディスク識別情報を有する該データ領域に記録することにより、該特定記録媒体を生成する特定記録媒体生成ステップとをそなえて構成されたことを特徴とする、請求項７又は請求項８に記載の記録媒体上での暗号化方法。

【請求項１０】　読み取り装置が読み出し可能な領域であってユーザはその領域をアクセスできない管理領域と、該読み取り装置が読み出し可能な領域であってユーザがその領域を任意にアクセスできるデータ領域とをそなえ、該管理領域に暗号化のためのディスク識別情報が記録された記録媒体における該ディスク識別情報を少なくとも読み出しうる読出手段と、

該データ領域に少なくとも上記のディスク識別情報を用いた暗号鍵によって音声、映像、データのいずれか一つの情報を含むメディア情報を暗号化して暗号化メディア情報として出力しうる暗号化メディア情報生成手段と、

該暗号化メディア情報を、同一のディスク識別情報を有する記録媒体の該データ領域に保存しうる暗号化メディア情報保存手段とをそなえて構成されたことを特徴とする、暗号化装置。

【請求項１１】　読み取り装置が読み出し可能な領域であってユーザはその領域をアクセスできない管理領域と、該読み取り装置が読み出し可能な領域であってユーザがその領域を任意にアクセスできるデータ領域とをそなえ、該管理領域に暗号化のためのディスク識別情報が記録されるとともに、該データ領域に暗号化された情報が記録された記録媒体における該ディスク識別情報を少なくとも読み出しうる第２読出手段と、

少なくとも該ディスク識別情報から第２暗号鍵を生成する第２暗号鍵生成手段と、

該暗号化された情報を該第２暗号鍵を用いて復号し、音

声、映像、データのいずれか一つの情報を含むメディア情報を再生しうる復号化手段とをそなえて構成されたことを特徴とする、復号化装置。

【請求項１２】　読み取り装置が読み出し可能な領域であってユーザはその領域をアクセスできない管理領域と、該読み取り装置が読み出し可能な領域であってユーザがその領域を任意にアクセスできるデータ領域とをそなえ、該管理領域に暗号化のためのディスク識別情報が記録された記録媒体における該ディスク識別情報を少なくとも読み出しうる読出手段と、

少なくとも該ディスク識別情報を用いた暗号鍵によって音声、映像、データのいずれか一つの情報を含むメディア情報を暗号化し暗号化メディア情報として出力しうる暗号化メディア情報生成手段と、

該暗号化メディア情報を該データ領域に保存しうる暗号化メディア情報保存手段とをそなえて構成されたことを特徴とする、音響・映像・データ装置。

【請求項１３】　読み取り装置が読み出し可能な領域であってユーザはその領域をアクセスできない管理領域と、該読み取り装置が読み出し可能な領域であってユーザがその領域を任意にアクセスできるデータ領域とをそなえ、該管理領域に暗号化のためのディスク識別情報が記録されるとともに、該データ領域に暗号化された情報が記録された記録媒体における該ディスク識別情報を少なくとも読み出しうる第２読出手段と、

少なくとも該ディスク識別情報から第２暗号鍵を生成する第２暗号鍵生成手段と、

該暗号化された情報を該第２暗号鍵を用いて復号し、音声、映像、データのいずれか一つの情報を含むメディア情報を再生しうる復号化手段とをそなえて構成されたことを特徴とする、音響・映像・データ装置。

【請求項１４】　該暗号化が、該ディスク識別情報，Ｑチャネルサブコードのモード２形式のフレームに記録された媒体識別番号情報並びにＱチャネルサブコードのモード３形式のフレームに記録されたシリアル番号情報又はこれらを組み合わせた情報を用いて行なわれることを特徴とする、請求項１～請求項４のいずれか一項に記載の記録媒体。

【請求項１５】　該暗号化が、該ディスク識別情報，Ｑチャネルサブコードのモード２形式のフレームに記録された媒体識別番号情報並びにＱチャネルサブコードのモード３形式のフレームに記録されたシリアル番号情報又はこれらを組み合わせた情報を種とする乱数関数を用いて行なわれることを特徴とする、請求項１～請求項４のいずれか一項に記載の記録媒体。

【請求項１６】　該暗号化が、ビット長を変化させうるキーメッセージ，該ディスク識別情報，Ｑチャネルサブコードのモード２形式のフレームに記録された媒体識別番号情報並びにＱチャネルサブコードのモード３形式のフレームに記録されたシリアル番号情報又はこれらを組

み合わせた情報を種とするハッシュ関数を用いて行なわれることを特徴とする、請求項１～請求項４のいずれか一項に記載の記録媒体。

【請求項１７】　該暗号化が、該ディスク識別情報，該媒体識別番号情報並びに該シリアル番号情報又はこれらを組み合わせた情報を用いて行なわれることを特徴とする、請求項６に記載の記録媒体の初期化方法。

【請求項１８】　該暗号化が、該ディスク識別情報，該媒体識別番号情報並びに該シリアル番号情報又はこれらを組み合わせた情報を用いて行なわれることを特徴とする、請求項８又は請求項９に記載の記録媒体上での暗号化方法。

【請求項１９】　該暗号化が、該ディスク識別情報，該媒体識別番号情報並びに該シリアル番号情報又はこれらを組み合わせた情報を種とする乱数関数を用いて行なわれることを特徴とする、請求項８又は請求項９に記載の記録媒体上での暗号化方法。

【請求項２０】　該暗号化が、ビット長を変化させうるキーメッセージ，該ディスク識別情報，該媒体識別番号情報並びに該シリアル番号情報又はこれらを組み合わせた情報を種とするハッシュ関数を用いて行なわれることを特徴とする、請求項８又は請求項９に記載の記録媒体上での暗号化方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＣＤ－Ｒ(CD-Recordable)、ＣＤ－ＲＷ(CD-Rewritable)、記録可能なＤＶＤ（Digital Versatile Disc）等に用いて好適な、記録媒体、記録媒体の初期化方法並びに記録媒体上での暗号化方法及び暗号化装置並びに復号化装置並びに音響・映像・データ装置に関する。

【０００２】

【従来の技術】近年、光学式にデータの書き込みが行なえるＣＤ－Ｒ（以下、ＣＤ－Ｒメディア又はＣＤ－Ｒディスクと称することがある），ＣＤ－ＲＷ（以下、ＣＤ－ＲＷメディア又はＣＤ－ＲＷディスクと称することがある）の製品開発がなされ、読み出し専用の音楽ＣＤやＣＤ－ＲＯＭ等に加えて、ＣＤ市場を活発化させている。

【０００３】これら一群は、ＣＤファミリと呼ばれ、ＣＤＤＡ，ＣＤ－ＭＩＤＩ，ＣＤＶ，ＣＤ－Ｇ，ＣＤ－ＲＯＭ等の種類がある。ここで、ＣＤＤＡは、いわゆる音楽ＣＤと呼ばれるものであって、ディジタルオーディオ信号の記録再生用である。また、ＣＤ－ＭＩＤＩ，ＣＤＶ，ＣＤ－Ｇは、パソコンの記録再生に用いられている。一方、ＣＤ－ＲＯＭは、読み出し専用メモリであって、これを応用したフォトＣＤ、ビデオＣＤ等も利用されている。

【０００４】これに対して、ＣＤ－ＲやＣＤ－ＲＷは、ユーザが書き込みをできるものである。これらの登場

で、ＣＤの作成は、オフィスや家庭においても行なえるようになった。ここで、ＣＤ－Ｒは、パソコンに搭載されているＣＤ－ＲＯＭドライブで再生可能なもので、大容量のデータを記録できる。その半面、１回しか書き込みできず、一旦記録されたデータの消去は行なえず、また、誤って書き込みしたディスクや、不要になったディスクを再利用することはできない。

【０００５】一方、ＣＤ－ＲＷは、ＣＤ－Ｒと異なり、データの書き換えが可能なものである。このＣＤ－ＲＷは、１０００回以上のデータの消去が可能で、大容量データの一時的な保存や、データの試し書きが行なえる。その半面、ディスクの価格がＣＤ－Ｒより高価で、記録されたディスクはＣＤ－ＲＷドライブ等の対応ドライブでしか再生できない。

【０００６】また、最近においては、ＣＤの数倍の容量をもつ読み出し専用のＤＶＤ（Digital Versatile Disc）やＤＶＤ－ＲＯＭが製品化されており、このような高密度媒体に対応したユーザが書き込み可能な媒体の開発が盛んに行なわれている。例えば、ＤＶＤ－Ｒなどの一度だけ書き込める媒体や、ＤＶＤ－ＲＡＭ，ＤＶＤ－ＲＷなどの１０００回以上書き換えられる媒体が開発されつつある。

【０００７】次に、ＣＤ－Ｒ／ＲＷを例として、そのデータの書き込みと、物理フォーマットとの手順を図２４から図２６を用いて説明する。なお、以下の説明中及び図面において、ＣＤ－ＲとＣＤ－ＲＷとの２つをまとめて呼称する際に、ＣＤ－Ｒ／ＲＷと表記することがある。図２４は、ＣＤ－Ｒ／ＲＷの非データ領域と、データ領域との配置を示す図である。この図２４に示すディスク６０は、管理領域６１と、ユーザ領域６２とをそなえてなる。

【０００８】この管理領域６１は、ユーザが、直接読み出しや書き込みをできない領域であり、この管理領域６１は、ＰＣＡ(Power Calibration Area)とＰＭＡ(Program Memory Area)とからなる。ここで、ＰＣＡは、データを書き込むときのレーザーの強さを調節するための制御情報が格納されている。そして、レーザーの強さは、このＰＣＡに記録された情報により、ＣＤ－Ｒディスクの色素や電源電圧、動作温度等の外部要因の変動等に合わせて最適化されている。

【０００９】また、ＣＤ－ＲディスクやＣＤ－ＲＷディスクのＰＭＡの一部には、最初に書き込みを行なう際に、ＣＤ－Ｒ／ＲＷドライブによって、個々のディスクを識別するためのディスクＩＤ（ディスク識別情報:Disc Identification）が、１０進数６桁、１９．９ビットで記録される。次に、ユーザ領域６２（図２４参照）は、音楽データ等の実際のデータが記録される領域である。

【００１０】そして、ユーザ領域６２は、さらに、リードイン領域６２ａと、データ領域６２ｂと、リードアウト領域６２ｃとからなる。ここで、データ領域６２ｂは、実際のデータの記録領域である。リードイン領域６２ａとリードアウト領域６２ｃとにはそれぞれ、このデータ領域６２ｂにデータを書き込む際の、データ開始点や停止点等の情報が記録されている。また、これらのリードイン領域６２ａとリードアウト領域６２ｃとが対になったもの（セッションという）が１つの単位として、データの書き込みが行なわれるようになっている。

【００１１】このディスクへの書き込みの方式は、ディスクアットワンス(Disk At Once)方式と、トラックアットワンス(Track At Once)方式と、パケットライト(PacketWrite)方式とがある。ディスクアットワンス方式とは、データが、ディスクの中心部から外周に向かって、一気に書き込まれる方式をいい、また、トラックアットワンス方式とは、まず、データが書き込まれ、その後、そのデータの前後に６０秒の制御情報（リードイン）と、９０秒又は３０秒の制御情報（リードアウト）とが付加される方式をいう。そして、パケットライト方式とは、トラックアットワンス方式をさらに進めて、短いデータ単位で記録を繰り返すことができる方式をいい、ＣＤ－Ｒでは、データは、前回書き込まれたデータの後ろに、引き続いて記録されるが、ＣＤ－ＲＷでは、フロッピー（登録商標）ディスク等と同様に、ディスクの各場所に、離散的に（とびとびに）記録が行なえる。

【００１２】ディスクアットワンス方式で書き込むと、ＣＤ－Ｒ／ＲＷディスクに空き容量があっても、残りの部分にデータを書き込むことができないので、ＣＤ－Ｒ／ＲＷディスクに空き容量が残っている場合、データの追記ができるように、トラックアットワンス方式又はパケットライト方式が好ましく用いられる。また、トラックアットワンス方式に類似のもので、リードイン，データ，リードアウトを、この順に記録するセッションアットワンス(Session At Once)方式も、最近認知されてきている。

【００１３】上記のリードイン領域６２ａは、ＣＤ－Ｒ上の各セッションの最初の領域に相当し、最初は何も書き込まれていない。また、セッションの書き込みが終了していない間は、ディスク上の次の書き込みアドレスが入れられ、そして、セッションの書き込みが終了するとＴＯＣが書き込まれる。このＴＯＣ(Table Of Contents)とは、ユーザ領域６２に書き込まれる情報であって、トラック番号，開始点，停止点の情報をいう。また、ＴＯＣは、ＣＤに記録されているトラック数や、それらの開始位置等が記録されるようになっていて、セッションの目次として機能している。

【００１４】さらに、リードアウト領域６２ｃは、セッションの最後にある領域で、データの最後に到達したことを示すのに用いられる。なお、データは何も書き込まれない。図２５は、書き込み途中におけるディスクのデータ構造を示す図である。この図２５の左側がディスク

６０の中心であり、この中心に一番近い方から、ＰＣＡ，ＰＭＡ，リードイン領域６２ａ，データ領域（プログラム領域）６２ｂ，リードアウト領域６２ｃが配置され、一番右側が外縁である。この図２５に示す網がけされた帯は、データが書き込まれていることを表しており、ＣＤ－Ｒの書き込み途中は、ＰＣＡ，ＰＭＡと、データ領域６２ｂとにデータが書き込まれ、トラック番号，開始点，停止点の情報が一時的に保存されるようになっている。

【００１５】図２６は、書き込み終了後におけるディスクのデータ構造を示す図であり、ディスク６０上のＰＣＡ，ＰＭＡには、何も書き込まれないが、リードイン領域６２ａには、ＴＯＣが書き込まれ、データ領域６２ｂには、音楽データ等が書き込まれ、さらに、リードアウト領域６２ｃに終了位置が書き込まれている。さて、上述した物理フォーマットに対して、データの記録は、ブロック（セクタ）単位で行なわれている。次に、この論理フォーマットについて図２７から図３８を用いて説明する。

【００１６】図２７は、サブコーディングフレームのフォーマットを示す図である。この図２７に示すブロック（セクタ）５３は、９８個のフレーム５３ａから構成されている。そして、ブロック５３は、サブコーディング領域５４と、データ領域５４ａとを有する。ここで、データ領域５４ａは、音楽等のデータが記録される領域である。

【００１７】また、サブコーディング領域５４は、無音部分，曲の楽章番号，インデックス，時間，文字等の情報を記録する領域であり、データ領域６２ｂ（図２４参照）に、音楽等のデータとともに、記録されるものである。このサブコーディング領域５４は、単独（一区切り毎）では用いられず、連続する９８フレームで１つの情報が表されるようになっている。

【００１８】また、図２８は、フレーム５３ａの詳細なフォーマットを示す図であり、この図２８に示すフレーム５３ａは、フレーム同期信号，サブコーディング，データ，パリティ，データ，パリティの各領域を有する。そして、１バイトのサブコーディング用の領域と、２４バイトのデータ用の領域とを有する。そして、このフレーム５３ａが、９８個集まって、２３５２（２４×９８）バイトのブロック５３が構成され、無音部分，曲の楽章番号，インデックス，時間，文字等の情報領域として機能するようになっている。

【００１９】図２９は、このサブコーディング領域を詳細に示した図である。この図２９に示すサブコーディング領域５４は、最初の２バイトの領域に、同期信号が格納され、その他の領域に、情報が記録されている。これらのチャネルは、具体的には、次のようになる。すなわち、Ｐチャネルは、曲と曲との間に挿入されている無音部分が記録されている。Ｑチャネルは、曲の楽章番号、楽章内のインデックス番号、曲のそのフレームにおける経過時間及び絶対時間などが記録されている。また、Ｒ，Ｓ，Ｔ，Ｕ，Ｖ，Ｗは、カラオケの表示用の文字情報等が記録されている。

【００２０】そして、この図２９に示す領域５４ｂのように、フレーム３からフレーム９８と付した縦方向の一束が、１チャネルを構成するようになっている。すなわち、Q1からQ96の９６ビットで、Ｑチャネルが形成される。また、Ｐ，Ｒ，Ｓ，Ｔ，Ｕ，Ｖ，Ｗの各チャネルも同様である。次に、Ｑチャネルのモードについて説明する。このＱチャネルは、モード１からモード３までの３種類のフォーマットの異なるモード形式を有する。Ｑチャネルは、通常は、モード１の形式を採るが、一定の頻度で、モード２，モード３の形式を採るようになっている。

【００２１】図３０は、Ｑチャネルのモード１のフレーム構造を示す図である。この図３０に示すモード１形式のフレーム５５によって、情報が伝達される。図３６は、データ記録の第１の例を示す図である。この図３６に示すように、Ｑチャネル領域は、モード１形式で記録され、そして、データ領域には、データが格納される。図３１は、Ｑチャネルのモード２のフレーム構造を示す図である。この図３１に示すモード２のフレーム５６は、フレーム５５と異なる形式であり、また、このフレーム５６が現れる頻度は、Ｑチャネルのうち、少なくとも１００ブロックに１ブロックの割合である。そして、この図３１のＮ１～Ｎ１３はそれぞれ、４ビットからなる領域であり、これらの領域Ｎ１～Ｎ１３に、ＭＣＮ（Media Catalog Number）が、１０進数１３桁（４３．２ビット）で記録される。このＭＣＮとは、メディア番号の識別子である。また、図３２は、ドライブ装置がＭＣＮを記録する際のデータフォーマットを示す図であり、このデータフォーマットに従って、ドライブ装置が記録を行なうと、実際には、ディスク上に図３１に示すフレーム構造が記録される。また、図３３は、ドライブ装置が読み込んだＭＣＮデータのフォーマットを示す図であり、フレーム構造を再生した際のデータフォーマットを示している。

【００２２】図３７は、データ記録の第２の例を示す図である。この図３７に示すように、Ｑチャネル領域のモード１形式の間に、モード２形式で、記録される。また、その場合のモード２形式のデータには、ＭＣＮ、例えば1234567890123 が格納される。図３４は、Ｑチャネルのモード３のフレーム構造を示す図である。この図３４に示すモード３のフレーム５７が現れる頻度も、Ｑチャネルうち、少なくとも１００ブロックに１ブロックである。そして、このフレーム５７のＩ１～Ｉ１２に、ＩＳＲＣ(International Standard Recoding Code)が、記録され、このうち、Ｉ８～Ｉ１２にシリアル番号(Serial Number）が、１０進数５桁（１６．６ビット）で記録

される。なお、Ｉ１～Ｉ５の領域は、６ビットで情報が記録され、Ｉ６～Ｉ１２の領域は、４ビットで情報が記録されるようになっている。また、図３５は、ドライブ装置が読み込んだＩＳＲＣデータのフォーマットを示す図であり、この図３５に示すＩ８～Ｉ１２の領域に、５桁分の１０進数でシリアル番号が書き込まれる。

【００２３】図３８は、データ記録の第３の例を示す図である。この図３８に示すように、Ｑチャネル領域のモード１形式の間にモード２形式で記録され、さらに、モード３形式でも記録されている。また、その場合のモード２形式のデータには、ＭＣＮ（例えば1234567890123）が書き込まれ、モード３形式のデータには、ＩＳＲＣのシリアル番号が例えば、98765 と書き込まれるようになっている。

【００２４】上述したように、ＣＤ－Ｒ／ＲＷは、そのフォーマット内容が、規格化されており、互換性に優れ、また、大変取扱いし易いものである。しかしながら、このＣＤ－Ｒ／ＲＷは、ユーザ個人が、簡単に、音楽や映画あるいはコンピュータプログラムのデータ等の著作物を複製できるので、このような著作物の保護が万全でないという課題がある。

【００２５】このような著作権付きのデータを保護する方法は、録音・再生機器に、使用料を予め上乗せする方法や、コピーするときのデータ列に暗号情報を乗せて行なう方法等がある。しかし、使用料を予め上乗せする方法は、料金の設定が大変難しいという課題があり、また、コピーするときのデータ列に暗号情報を乗せる方法は、アナログ的にコピーする場合には、何ら防止する手立てがないという課題があり、いずれも、複製防止のための根本的な解決とはなっていない。

【００２６】なお、データ記録に関しては、以下に示すような、例えば４種類の公知文献が知られている。まず、特開平８－１５３３３１号公報（以下、公知文献１と称することがある）には、コピープロテクトが可能なデータ構造を備えるＣＤ－ＲＯＭおよびコピー品ＣＤ－ＲＯＭの判別手段を得て、不正コピーの防止を図る技術が開示されている。

【００２７】しかしながら、この公知文献１に記載された技術は、媒体の特定部分を、コピー防止のための特定値としている。さらに、この技術は、例えばＣＤの任意のサブコードブロックのＱチャネルアドレスを特定値としているので、データ保護の信頼性が低いという課題がある。また、特開平７－８５５７４号公報（以下、公知文献２と称することがある）には、ソフトウエアや音楽情報を供給する光ディスクのコストアップをせずに、収録されたソフトウエアや音楽情報のコピー防止を行なう技術が開示されている。

【００２８】この公知文献２に記載された技術は、暗号化のキー情報を、バーコードなどにより非データ記録領域に記録することにより、コピーを防止していている。しかしながら、非データ領域は再生装置の光ヘッドが走査しない領域であり、また、キー情報はバーコードや幾何学模様で記録されているため、専用のキー情報読み取り手段が必要であるという課題がある。

【００２９】さらに、ＵＳＰ５，８０２，１７４（対応する日本出願は、特開平９－０１７１１９号公報、以下、公知文献３と称することがある）には、ピットでデータが記録されたＣＤ－ＲＯＭなどの媒体であって、簡単に複製されることなく、また、例えピット形成部分の複製ができたとしても、記録されている情報信号を容易に再生することができないようにすることが可能なデータ記録媒体等が開示されている。

【００３０】この公知文献３に記載された技術は、暗号化データと暗号化キー情報とを、記録形式または記録層が異なる２つの記録領域に別々に記録するものであって、例えば、暗号化キー情報を、溝のウォブルや、光磁気や相変化により記録したり、あるいは、他の記録層に記録したりする。しかしながら、この公知文献３に記載さえた技術はいずれも、ＣＤ－ＲＯＭなどＲＯＭ媒体のコピー防止技術であるため、本発明のような記録可能媒体への適用は困難である。

【００３１】さらに、暗号化キーを書き込む記録層を異ならせただけでは、暗号化キーの読み取りやコピーは容易にできてしまう。溝のウォブルにより暗号化キー情報を書き込むと、ディスク毎に異なる識別番号は付与できず、記録可能媒体でのコピー防止効果はない。また、光磁気などのピット以外の他の記録形式を用いて、暗号化キー情報を書き込むと、読み出すためには専用のキー情報読み取り手段が必要であるという課題がある。

【００３２】そして、ＥＰ７５１５１６Ａ（対応する日本出願は、特開平９－１１５２４１号公報、以下、公知文献４と称することがある）には、簡単に複製されることなく、また、複製されたとしても再生できないデータ記録装置が開示されている。しかしながら、この公知文献４に記載された技術は、媒体に固有の識別情報を記録するものであって、例えば、データ領域やＴＯＣ領域などにその識別情報が記録されるものである。従って、ＴＯＣ領域は、ユーザにより任意に書き換えされるので、やはり、ユーザによるデータの暗号化キーの改竄のおそれがあるという課題がある。

【００３３】

【発明が解決しようとする課題】本発明は、このような課題に鑑み創案されたもので、既存のフォーマット方法を利用してディスクに所定の初期化を施すことにより、ユーザが音楽や映画あるいはコンピュータプログラムのデータ等の著作権付きのデータを、１枚のディスクに１回だけコピーすることは可能であるが、そのコピーされたディスクから他のディスクへ二次コピーすることはできないような、記録媒体、記録媒体の初期化方法並びに記録媒体上での暗号化方法及び暗号化装置並びに復号化

装置並びに音響・映像・データ装置を提供することを目的とする。

【００３４】

【課題を解決するための手段】このため、本発明の記録媒体は、読み取り装置が読み出し可能な領域であってユーザはその領域をアクセスできない管理領域と、読み取り装置が読み出し可能な領域であってユーザがその領域を任意にアクセスできるデータ領域とをそなえ、その管理領域に、暗号化のためのディスク識別情報が記録されていることを特徴としている（請求項１）。

【００３５】また、そのデータ領域に、音声、映像、データのいずれか一つの情報を含むメディア情報が、少なくとも上記のディスク識別情報を用いて生成された暗号鍵によって暗号化された暗号化メディア情報として記録されるとともに、ユーザが読み出しうる媒体識別番号情報が、分散されて記録されてもよく、また、この記録媒体が、光学式に記録されるようにしてもよく、そのデータ領域が、ユーザによって少なくとも１回は書き込まれ得るようにしてもよい（請求項２～４）。

【００３６】加えて、この暗号化は、ディスク識別情報，Ｑチャネルサブコードのモード２形式のフレームに記録された媒体識別番号情報並びにＱチャネルサブコードのモード３形式のフレームに記録されたシリアル番号情報又はこれらを組み合わせた情報を用いて行なわれるようにしてもよく（請求項１４）、ディスク識別情報，Ｑチャネルサブコードのモード２形式のフレームに記録された媒体識別番号情報並びにＱチャネルサブコードのモード３形式のフレームに記録されたシリアル番号情報又はこれらを組み合わせた情報を種とする乱数関数を用いて行なわれるようにしてもよく（請求項１５）、また、ビット長を変化させうるキーメッセージ，ディスク識別情報，Ｑチャネルサブコードのモード２形式のフレームに記録された媒体識別番号情報並びにＱチャネルサブコードのモード３形式のフレームに記録されたシリアル番号情報又はこれらを組み合わせた情報を種とするハッシュ関数を用いて行なわれるようにしてもよい（請求項１６）。

【００３７】さらに、本発明の記録媒体の初期化方法は、読み取り装置が読み出し可能な領域であってユーザはその領域をアクセスできない管理領域と、読み取り装置が読み出し可能な領域であってユーザがその領域を任意にアクセスできるデータ領域とをそなえた記録媒体の初期化方法であって、管理領域に暗号化のためのディスク識別情報を記録することを特徴としている（請求項５）。

【００３８】そして、上記のディスク識別情報を記録するに当たり、管理領域に暗号化のためのディスク識別情報を記録する第１書込ステップと、データ領域にＱチャネルサブコードのモード２形式で媒体識別番号情報を記録する第２書込ステップと、データ領域にＱチャネルサブコードのモード３形式でシリアル番号情報を記録する第３書込ステップとをそなえて構成されてもよい（請求項６）。

【００３９】加えて、この暗号化は、ディスク識別情報，Ｑチャネルサブコードのモード２形式のフレームに記録された媒体識別番号情報並びにＱチャネルサブコードのモード３形式のフレームに記録されたシリアル番号情報又はこれらを組み合わせた情報を用いて行なわれるようにしてもよく（請求項１７）、ディスク識別情報，Ｑチャネルサブコードのモード２形式のフレームに記録された媒体識別番号情報並びにＱチャネルサブコードのモード３形式のフレームに記録されたシリアル番号情報又はこれらを組み合わせた情報を種とする乱数関数を用いて行なわれるようにしてもよく、また、ビット長を変化させうるキーメッセージ，ディスク識別情報，Ｑチャネルサブコードのモード２形式のフレームに記録された媒体識別番号情報並びにＱチャネルサブコードのモード３形式のフレームに記録されたシリアル番号情報又はこれらを組み合わせた情報を種とするハッシュ関数を用いて行なわれるようにしてもよい。

【００４０】加えて、本発明の記録媒体上での暗号化方法は、読み取り装置が読み出し可能な領域であってユーザはその領域をアクセスできない管理領域と、読み取り装置が読み出し可能な領域であってユーザがその領域を任意にアクセスできるデータ領域とをそなえた記録媒体上での暗号化方法であって、管理領域に暗号化のためのディスク識別情報を記録する初期化を行なった後に、音声、映像、データのいずれか一つの情報を含むメディア情報を、少なくとも上記のディスク識別情報を用いた暗号鍵によって暗号化し、暗号化メディア情報としてデータ領域に記録することにより、特定記録媒体を生成する暗号化ステップをそなえて構成されたことを特徴としている（請求項７）。

【００４１】そして、上記の初期化は、管理領域に暗号化のためのディスク識別情報を記録する第１書込ステップと、データ領域にＱチャネルサブコードのモード２形式で媒体識別番号情報を記録する第２書込ステップと、データ領域にＱチャネルサブコードのモード３形式でシリアル番号情報を記録する第３書込ステップとから構成されてもよい（請求項８）。

【００４２】また、その暗号化ステップが、ディスク識別情報を第１ディスク識別情報として読み出す第１ディスク識別情報読出ステップと、第１ディスク識別情報と、媒体識別番号情報及びシリアル番号情報のうちの少なくとも一つの情報とを組み合わせて第１暗号鍵を生成する第１暗号鍵生成ステップと、外部装置よりメディア情報を読み出す第１読出ステップと、第１暗号鍵を用いて暗号化メディア情報を生成し、第１ディスク識別情報を有するデータ領域に記録することにより、特定記録媒体を生成する特定記録媒体生成ステップとをそなえて構

成されてもよい（請求項９）。

【００４３】加えて、この暗号化は、ディスク識別情報，媒体識別番号情報並びにシリアル番号情報又はこれらを組み合わせた情報を用いて行なわれるようにしてもよく（請求項１８）、ディスク識別情報，媒体識別番号情報並びにシリアル番号情報又はこれらを組み合わせた情報を種とする乱数関数を用いて行なわれるようにしてもよく（請求項１９）、また、ビット長を変化させうるキーメッセージ，ディスク識別情報，媒体識別番号情報並びにシリアル番号情報又はこれらを組み合わせた情報を種とするハッシュ関数を用いて行なわれるようにしてもよい（請求項２０）。

【００４４】さらに、本発明の暗号化装置は、読み取り装置が読み出し可能な領域であってユーザはその領域をアクセスできない管理領域と、読み取り装置が読み出し可能な領域であってユーザがその領域を任意にアクセスできるデータ領域とをそなえ、管理領域に暗号化のためのディスク識別情報が記録された記録媒体におけるディスク識別情報を少なくとも読み出しうる読出手段と、データ領域に少なくとも上記のディスク識別情報を用いた暗号鍵によって音声、映像、データのいずれか一つの情報を含むメディア情報を暗号化して暗号化メディア情報として出力しうる暗号化メディア情報生成手段と、暗号化メディア情報を、同一のディスク識別情報を有する記録媒体のデータ領域に保存しうる暗号化メディア情報保存手段とをそなえて構成されたことを特徴としている（請求項１０）。

【００４５】加えて、この暗号化は、ディスク識別情報，Ｑチャネルサブコードのモード２形式のフレームに記録された媒体識別番号情報並びにＱチャネルサブコードのモード３形式のフレームに記録されたシリアル番号情報又はこれらを組み合わせた情報を用いて行なわれるようにしてもよく、ディスク識別情報，Ｑチャネルサブコードのモード２形式のフレームに記録された媒体識別番号情報並びにＱチャネルサブコードのモード３形式のフレームに記録されたシリアル番号情報又はこれらを組み合わせた情報を種とする乱数関数を用いて行なわれるようにしてもよく、また、ビット長を変化させうるキーメッセージ，ディスク識別情報，Ｑチャネルサブコードのモード２形式のフレームに記録された媒体識別番号情報並びにＱチャネルサブコードのモード３形式のフレームに記録されたシリアル番号情報又はこれらを組み合わせた情報を種とするハッシュ関数を用いて行なわれるようにしてもよい。

【００４６】そして、本発明の復号化装置は、読み取り装置が読み出し可能な領域であってユーザはその領域をアクセスできない管理領域と、読み取り装置が読み出し可能な領域であってユーザがその領域を任意にアクセスできるデータ領域とをそなえ、管理領域に暗号化のためのディスク識別情報が記録されるとともに、データ領域

に暗号化された情報が記録された記録媒体におけるディスク識別情報を少なくとも読み出しうる第２読出手段と、少なくともディスク識別情報から第２暗号鍵を生成する第２暗号鍵生成手段と、暗号化された情報を第２暗号鍵を用いて復号し、音声、映像、データのいずれか一つの情報を含むメディア情報を再生しうる復号化手段とをそなえて構成されたことを特徴としている（請求項１１）。

【００４７】加えて、この暗号化は、ディスク識別情報，Ｑチャネルサブコードのモード２形式のフレームに記録された媒体識別番号情報並びにＱチャネルサブコードのモード３形式のフレームに記録されたシリアル番号情報又はこれらを組み合わせた情報を用いて行なわれるようにしてもよく、ディスク識別情報，Ｑチャネルサブコードのモード２形式のフレームに記録された媒体識別番号情報並びにＱチャネルサブコードのモード３形式のフレームに記録されたシリアル番号情報又はこれらを組み合わせた情報を種とする乱数関数を用いて行なわれるようにしてもよく、また、ビット長を変化させうるキーメッセージ，ディスク識別情報，Ｑチャネルサブコードのモード２形式のフレームに記録された媒体識別番号情報並びにＱチャネルサブコードのモード３形式のフレームに記録されたシリアル番号情報又はこれらを組み合わせた情報を種とするハッシュ関数を用いて行なわれるようにしてもよい。

【００４８】加えて、本発明の音響・映像・データ装置は、読み取り装置が読み出し可能な領域であってユーザはその領域をアクセスできない管理領域と、読み取り装置が読み出し可能な領域であってユーザがその領域を任意にアクセスできるデータ領域とをそなえ、管理領域に暗号化のためのディスク識別情報が記録された記録媒体におけるディスク識別情報を少なくとも読み出しうる読出手段と、少なくともディスク識別情報を用いた暗号鍵によって音声、映像、データのいずれか一つの情報を含むメディア情報を暗号化し暗号化メディア情報として出力しうる暗号化メディア情報生成手段と、暗号化メディア情報をデータ領域に保存しうる暗号化メディア情報保存手段とをそなえて構成されたことを特徴としている（請求項１２）。

【００４９】また、本発明の音響・映像・データ装置は、読み取り装置が読み出し可能な領域であってユーザはその領域をアクセスできない管理領域と、読み取り装置が読み出し可能な領域であってユーザがその領域を任意にアクセスできるデータ領域とをそなえ、管理領域に暗号化のためのディスク識別情報が記録されるとともに、データ領域に暗号化された情報が記録された記録媒体におけるディスク識別情報を少なくとも読み出しうる第２読出手段と、少なくともディスク識別情報から第２暗号鍵を生成する第２暗号鍵生成手段と、暗号化された情報を第２暗号鍵を用いて復号し、音声、映像、データ

のいずれか一つの情報を含むメディア情報を再生しうる復号化手段とをそなえて構成されたことを特徴としている（請求項１３）。

【００５０】加えて、この暗号化は、ディスク識別情報，Ｑチャネルサブコードのモード２形式のフレームに記録された媒体識別番号情報並びにＱチャネルサブコードのモード３形式のフレームに記録されたシリアル番号情報又はこれらを組み合わせた情報を用いて行なわれるようにしてもよく、ディスク識別情報，Ｑチャネルサブコードのモード２形式のフレームに記録された媒体識別番号情報並びにＱチャネルサブコードのモード３形式のフレームに記録されたシリアル番号情報又はこれらを組み合わせた情報を種とする乱数関数を用いて行なわれるようにしてもよく、また、ビット長を変化させうるキーメッセージ，ディスク識別情報，Ｑチャネルサブコードのモード２形式のフレームに記録された媒体識別番号情報並びにＱチャネルサブコードのモード３形式のフレームに記録されたシリアル番号情報又はこれらを組み合わせた情報を種とするハッシュ関数を用いて行なわれるようにしてもよい。

【００５１】

【発明の実施の形態】以下、ＣＤ－Ｒ／ＲＷを例とし、図面を参照して本発明の実施の形態を説明する。

（Ａ）本発明の第１実施形態の説明

図１は、本発明が適用される、ＣＤ－Ｒ／ＲＷの非データ領域と、データ領域との配置を示す図である。この図１に示すディスク１０は、光学式に読み出し又は書き込み可能な記録媒体であって、管理領域１１と、ユーザ領域１２とをそなえている。また、このディスク１０は、初期化される前のものである。

【００５２】ここで、初期化とは、物理的な円盤（ディスク又はメディアと称することがある）に、ディスクＩＤ，ＭＣＮ，ＩＳＲＣ等を刷り込む（記録する）ことをいう。また、その初期化された円盤を使用する態様は、産業用と民生用とがある。すなわち、産業用とは、例えば、一次メーカーがこの物理的な円盤に初期化を施して販売し、二次メーカーがその初期化された物理的な円盤を購入して、音声，映像，データ等を記録して販売することをいう。また、民生用とは、例えば、一般消費者が初期化された円盤を購入して、音声，映像，データ等を個人レベルで記録することをいう。従って、以下、ユーザという語は、その二次メーカーや、一般消費者等を意味する。なお、このディスク１０は、具体的には、１回しか書き込みできないＣＤ－Ｒ又は、何回もデータの書き換えが可能なＣＤ－ＲＷである。

【００５３】この管理領域１１は、ドライブ装置（図示せず）が読み出し可能な領域であってユーザはその領域をアクセスできない領域であり、ＰＣＡとＰＭＡとからなる。ここで、ドライブ装置とは、ＣＤ－Ｒ／ＲＷの再生装置又は記録装置内にある読み取り装置である。すなわち、ユーザが使用する民生用の再生装置等に内蔵するドライブ装置は、この管理領域１１を読み出すことが可能であるが、ユーザは、この管理領域１１の値を任意には書き換えたり、消去したりすることはできないようになっている。すなわち、ユーザが任意に書き換えたり、消去したりするためのコマンドが存在しない領域である。また、ＰＣＡは、データを書き込むときのレーザーの強さを調節するための情報が記録されている領域である。

【００５４】さらに、ＰＭＡは、暗号化のためのディスクＩＤ（ディスク識別情報）が記録される領域であり、このディスクＩＤにより、個々のディスクが識別されるようになっている。また、このディスクＩＤは、ディスクを初期化する際に、ドライブ装置によって、ほぼランダムに番号を設定して書き込まれるものであり、さらに、特殊な装置でない限り、このディスクＩＤを特定の番号に設定することはできない。従って、家庭やオフィスで使用するユーザは、そのような特殊な装置を有しないので、このディスクＩＤを特定の番号には書き換えられないようになっている。

【００５５】なお、管理領域１１は、通常、最内周に１カ所設けられ、容量はごく少なくデータ記録容量の１％以下である。さらに、ユーザ領域１２は、ドライブ装置が読み出し可能な領域であってユーザがその領域を任意にアクセスできる領域である。このユーザ領域１２は、リードインを格納するためのリードイン領域１２ａと、音楽等のデータを格納するためのデータ領域（プログラム領域）１２ｂと、リードアウトを格納するためのリードアウト領域１２ｃとからなる。

【００５６】そして、音声、映像、データ等のマルチメディアデータは、このデータ領域１２ｂに、ディスクＩＤ，ＭＣＮ（媒体識別番号情報），ＩＳＲＣのシリアル番号（シリアル番号情報）を用いて生成された暗号化キー（暗号鍵）によって暗号化され、暗号化データ（暗号化メディア情報）として記録されるとともに、ユーザが読み出しうるＭＣＮ，ＩＳＲＣのシリアル番号が、このデータ領域１２ｂに、分散されて記録されるようになっている。すなわち、ユーザが音楽データを書き込みを行なう際に、無音部分，曲の楽章番号，インデックス，時間，文字等のデータが、音楽データとともに、データ領域１２ｂ中のサブコーディング用の領域に、書き込まれる。なお、ＣＤ－Ｒのデータ領域１２ｂは、ユーザによって１回のみ書き込まれ、ＣＤ－ＲＷのデータ領域１２ｂは、ユーザによって、何回でも書き換え可能である。

【００５７】ここで、ＭＣＮは、メディア番号の識別子であって、そのサブコーディング用の領域中のＱチャネル（モード２形式）で記録された情報である。さらに、ＩＳＲＣのシリアル番号は、サブコーディング用の領域中のＱチャネル（モード３形式）で記録された情報である。図２（ａ）は、初期化されたＣＤ－Ｒ／ＲＷの概念

17

的な領域配置を示す図である。この図２（ａ）に示すディスク１０は、データ領域１２ｂと、メディア番号領域１とを有する。なお、ディスク１０の中心部の穴は、省略している。

【００５８】ここで、メディア番号領域１は、上記のディスクＩＤ，ＭＣＮ，ＩＳＲＣの３領域を寄せ集めた概念的な領域であり、実際には、このような形で、ディスク１０の領域が使用されているわけではない。また、これらの長さは、ディスクＩＤが１０進数の６桁で、ＭＣＮが１０進数１３桁で、ＩＳＲＣのシリアル番号が１０進数５桁であり、これらが、適当に組み合わされて暗号化キーとして用いられるようになっている。なお、その組み合わせについては、後述する。

【００５９】そして、マルチメディアデータは、これらの刷り込まれたディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号を組み合わせたメディア番号により、暗号化されるようになっている。あるいは、ＩＳＲＣのシリアル番号の代わりに、ＩＳＲＣ全体を用いてもよい。図２（ｂ）は、暗号化データが記録されたＣＤ－Ｒ／ＲＷの概念的な領域配置を示す図であり、この図２（ｂ）に示すディスク１０′は、メディア番号領域１と暗号化データ１４とが記録されている。すなわち、マルチメディアデータは、メディア番号を暗号化キーとして用いて暗号化され、図２（ｂ）に示す暗号化データ１４が得られるようになっている。

【００６０】図３は、メディア番号により暗号化されることを説明するための図である。この図３に示すデータ１３（図３の左側の円形のもの）は、暗号化されていないデータであり、具体的には、音声、映像、データ等の情報を含むマルチメディアデータである。そして、このデータ１３が、ディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号からなるメディア番号（メディア番号領域）１を用いた暗号化キーによって暗号化され、この図３に示すように、暗号化データ１４（図３の右側の円形のもの）が得られる。さらに、この暗号化データ１４が記録されたものが、特定ディスク１０′として生成されるのである（暗号化ステップ）。すなわち、メディア番号（メディア番号領域）１が、ディスク１枚毎に異なる固有なものなので、暗号化キーとして機能しているのである。

【００６１】従って、本発明の記録媒体上での暗号化方法は、ドライブ装置（図示省略）が読み出し可能な領域であってユーザはその領域をアクセスできない管理領域１１と、ドライブ装置が読み出し可能な領域であってユーザがその領域を任意にアクセスできるデータ領域１２ｂとをそなえたディスク１０上での暗号化方法であって、管理領域１１に暗号化のためのディスクＩＤを記録する初期化を行なった後に、音声、映像、データのいずれか一つの情報を含むメディア情報を、上記のディスクＩＤを用いた暗号キーによって暗号化し、暗号化メディア情報としてデータ領域１２ｂに記録することにより、特定ディスク１０′を生成する暗号化ステップとをそなえて構成されたことになる。

18

【００６２】ここで、図８を用いて後述するように、上記の初期化は、管理領域１１に暗号化のためのディスクＩＤを記録する第１書込ステップと、データ領域１２ｂにＱチャネルサブコードのモード２形式でディスクＩＤ，ＭＣＮ（媒体識別番号情報）を記録する第２書込ステップと、データ領域１２ｂにＱチャネルサブコードのモード３形式でＩＳＲＣのシリアル番号（シリアル番号情報）を記録する第３書込ステップとからなる。

【００６３】具体的には、この暗号化ステップは、まず、ディスクＩＤが第１ディスク識別情報として読み出される（第１ディスク識別情報読出ステップ）。さらに、そのディスクＩＤとＭＣＮとの組み合わせ、ディスクＩＤとＩＳＲＣのシリアル番号との組み合わせ、あるいは、ディスクＩＤとＭＣＮとＩＳＲＣのシリアル番号との組み合わせでメディア番号１が生成される（第１暗号鍵生成ステップ）。そして、外部装置よりデータ１３が読み出され（第１読出ステップ）、メディア番号１を用いて暗号化データ１４が生成され、同じディスクＩＤを有するディスク１０のデータ領域１２ｂに記録されることにより、特定ディスク１０′が生成されるのである（特定記録媒体生成ステップ）。

【００６４】図４は、メディア番号により復号化されることを説明するための図である。この図４に示す暗号化データ１４は、メディア番号（メディア番号領域）１′によって復号（復元）され、元のデータ１３が得られる。すなわち、復号化ステップは、まず、特定ディスク１０′のディスクＩＤが第２ディスク識別情報として読み出される。そして、この特定ディスク１０′から暗号化データ１４が読み出され、そのディスクＩＤとＭＣＮとの組み合わせ、ディスクＩＤとＩＳＲＣのシリアル番号との組み合わせ及びディスクＩＤとＭＣＮとＩＳＲＣのシリアル番号との組み合わせからメディア番号（メディア番号領域）１′が生成される。すなわち、メディア番号（メディア番号領域）１′は、第２暗号鍵として機能している。ここで、メディア番号１′がメディア番号１と一致する場合のみ、暗号化データ１４は復号されて再現できるのである。

【００６５】図５は、二次コピーができないことを説明するための図である。図５には、ディスク１０′とディスク１０ａとの２種類の異なるものが示されている。ここで、ディスク１０′は、例えば、音楽ＣＤから一次コピーされたディスクである。一方、ディスク１０ａは、初期化された別のディスクであって、一次コピーされたディスク１０′から、さらに、二次コピーされたものである。

【００６６】ここで、ＣＤ－Ｒ／ＲＷドライブ（後述）によって、二次コピーされたデータを読み出しても、暗

19

号化キーであるメディア番号１とメディア番号１′とが、異なるので、このコピーされたディスク１０ａの暗号化データ１４は、復号されないのである。このように、メディア番号を用いた暗号化キーは、一通りになるので、二次コピーが防止される。また、このように、ＣＤ－ＲディスクあるいはＣＤ－ＲＷディスク内の管理領域１１とデータ領域１２ｂとを利用して、これらの領域に暗号化キーとなるデータが分散されて記録され、その分散されて記録されたデータを寄せ集めて暗号化キーが生成されている。従って、この方法によれば、既存のディスクのフォーマット方法を変更せずに、暗号化が行なえるようになる。加えて、分散方法は、必要に応じて、種々に変更させることができるので、暗号化キーとしての強度を高めることができるのである。

【００６７】次に、暗号化キーであるメディア番号について、具体的に説明する。よく知られているように、暗号化方法には、暗号化キーと復号化キーとが同一の対称法と、暗号化キーと復号化キーとが同一でない非対称法とがある。前者を用いた例は、ＤＥＳ（Data Encryption Standard），ＲＣ４(Rivest Code #4)，ＩＤＥＡ等があり、後者を用いた例は、ＲＳＡ（Rivest, Shamit, Adleman）等がある。

【００６８】図６は、暗号化キーを用いた暗号化方法を示す図である。この図６に示すように、元のデータ"ABCD"は、" 暗号化キー " を掛け合わされて、暗号化データ"????"が得られる。そして、暗号化データ"????"は、" 復号化キー " を掛け合わされて、元のデータ"ABCD"が得られるようになっている。そして、通常使われる暗号化キーの長さはそれぞれ、ＤＥＳが５６ビット、ＲＣ４が４６～１２８ビット、ＩＤＥＡが１２８ビットであり、また、ＲＳＡは、５１２～４０９６ビットである。なお、この５６ビットのＤＥＳと、１０２４ビットのＲＳＡとは、その復号の難度が同程度である。

【００６９】ところで、上記のメディア番号を用いて暗号化する場合、メディア番号は、その暗号化に必要な数のビットを有していなければならない。一方、ＭＣＮは１０進数１３桁（２進数４３．２ビット）で、ＩＳＲＣは１０進数５桁（２進数１６．６ビット）で、また、ディスクＩＤは１０進数６桁（２進数１９．９ビット）である。これら単体では、十分な長さの暗号を作成することはできない。従って、これら３種類を、使用する暗号化方法に応じて、上記の３種類の暗号化キー１～３を組み合わせるようにするのである。次に、（ｉ）から（ｖｉ）に、暗号化キー１～３の使用例を示す。なお、以下の説明においては、ＭＣＮを暗号化キー１、ＩＳＲＣのシリアル番号を暗号化キー２、また、ディスクＩＤを暗号化キー３と称して説明することがある。

（ｉ）暗号化キーの長さが１０進数６桁で十分な場合
暗号化キー３（１０進数６桁）を使用。

（ｉｉ）暗号化キーの長さが１０進数１１桁で十分な場合
暗号化キー２（１０進数５桁）と暗号化キー３（１０進数６桁）とを使用。

（ｉｉｉ）暗号化キーの長さが１０進数１９桁で十分な場合
暗号化キー１（１０進数１３桁）と暗号化キー３（１０進数６桁）とを使用。

（ｉｖ）暗号化キーの長さが１０進数２４桁で十分な場合
暗号化キー１（１０進数１３桁）と暗号化キー２（１０進数５桁）と暗号化キー３（１０進数６桁）とを使用。

（ｖ）暗号化キーの長さが（ｉｖ）よりも大きい場合
暗号化キー１と暗号化キー２と暗号化キー３とに加えて、データ部分に不足しているだけの暗号化キーを作成して使用する。例えば３０桁必要の場合は、いずれかの適当なフォーマット部分から、他の６桁を取得するようにしたり、あるいは、その６桁をデータ部分に書き込んでもよい。

（ｖｉ）暗号化キーの長さが（ｉｖ）よりも大きい場合であって、ＣＤ－Ｒディスクである場合
複数のトラックを作成することにより、複数の暗号化キー１と暗号化キー２とをそれぞれ作成しておき、これら複数の暗号化キー１，２と、暗号化キー３とを併せて使用する。

【００７０】また、データの暗号化においては、暗号化キーの秘匿性を高めなければならない。その場合は、ＭＣＮ（暗号化キー１），ＩＳＲＣのシリアル番号（暗号化キー２），ディスクＩＤ（暗号化キー３）の３種類が、それぞれ、特定の関数に代入されて計算され、その計算された結果が暗号化キーとして使用されるのである。この特定の関数として採用されるためには、次の①，②の条件が満たされる必要がある。

【００７１】①同一のＭＣＮ，ＩＳＲＣのシリアル番号，ディスクＩＤからは同一の結果が得られること。
②逆解析されにくいこと。
この①の条件は、真の乱数を発生する関数を用いると、毎回異なる結果が現れてしまい、一定の暗号化キーを再生できなくなるからである。また、②の条件は、計算された結果から、逆関数を用いて、元のＭＣＮ，ＩＳＲＣのシリアル番号，ディスクＩＤが、それぞれ、解読されないようにするためである。これら３種類の暗号化キーを便宜上ＩＤと称して、暗号化キーを生成するアルゴリズムを、図３９（ａ）～（ｃ）を用いて説明する。

【００７２】図３９（ａ）は、３種類の暗号化キー１～３を単純加算した暗号化キー生成方法の説明図であり、図３９（ｂ）は、３種類の暗号化キー１～３をそれぞれ乱数関数を用いた暗号化キー生成方法の説明図であり、また、図３９（ｃ）は、キーメッセージと３種類の暗号化キー１～３とをハッシュ関数を用いた暗号化キー生成方法の説明図である。なお、これらの図において、暗号

化キーはユニークＩＤとも表示され、また、暗号化キー１（ＭＣＮ）はＩＤ１，暗号化キー２（ＩＳＲＣのシリアル番号）はＩＤ２，暗号化キー３（ディスクＩＤ）はＩＤ３と、それぞれ表示されている。

【００７３】ここで、図３９（ａ）に示すＣａｓｅ１は、上述した（ｉｖ）～（ｖｉ）に相当するものであって、暗号化キー（ユニーク　ＩＤ）が、暗号化キー１（ＩＤ１），暗号化キー２（ＩＤ２），暗号化キー３（ＩＤ３）の３種類のものが加算されて生成されるようになっている。また、必要な暗号化キーの長さが短い場合には、上述した（ｉ）～（ｉｉｉ）に相当し、ＭＣＮ，ＩＳＲＣのシリアル番号，ディスクＩＤを個別に用いてもよい。従って、この暗号化は、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号又はこれらを組み合わせた情報を用いて行なわれていることになる。そして、その組み合わせ方は、ＭＣＮ，ＩＳＲＣのシリアル番号，ディスクＩＤの３種類から、６通りある。

【００７４】次に、図３９（ｂ）に示すＣａｓｅ２では、暗号化キー（ユニーク　ＩＤ）が、ＭＣＮ（ＩＤ１）を種として発生させた乱数関数Ｒｎｄ（ＩＤ１）の結果と、ＩＳＲＣのシリアル番号（ＩＤ２）を種として発生させた乱数関数Ｒｎｄ（ＩＤ２）の結果と、ディスクＩＤ（ＩＤ３）を種として発生させた乱数関数Ｒｎｄ（ＩＤ３）の結果とが、加算されて得られるようになっている。

【００７５】ここで、乱数関数Ｒｎｄ（）とは、入力された種を基に疑似乱数を発生させる関数であり、この乱数関数Ｒｎｄ（）は、例えば、種として入力された数に対して、非常に大きい整数を乗算し、その乗算結果に非常に大きい整数を加算し、さらに、その加算結果の所定の桁における値を出力するようになっている。また、種とは、その乱数関数Ｒｎｄ（）内部での乱数発生演算を行なうための、初期値を意味する。

【００７６】従って、この暗号化は、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を種とする乱数関数を用いてなされたことになり、また、この暗号化は、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を組み合わせた情報を種とする乱数関数を用いてなされていることになる。実用上は、同一のＭＣＮ，同一のＩＳＲＣのシリアル番号，同一のディスクＩＤを用いて暗号化キーを生成するときに、同一の結果が出力されるように、乱数関数Ｒｎｄ（）は、固定の乱数表を予め用意しておき、同一のＭＣＮ，同一のＩＳＲＣのシリアル番号，同一のディスクＩＤに対しては、特定の数字を出力するようになっている。なお、ＭＣＮ，ＩＳＲＣのシリアル番号，ディスクＩＤの３種類の全てを加算し、その加算結果を種として乱数関数Ｒｎｄ（）に代入するようにしてもよい。

【００７７】このように、アルゴリズムにおいて、乱数関数Ｒｎｄ（）が用いられるので、同一の暗号化キーが出力されるようになり、また、その生成された暗号化キーは、逆解析がされにくい。加えて、図３９（ｃ）に示したＣａｓｅ３では、暗号化キー（ユニーク　ＩＤ）が、可変長のキーメッセージと、ＭＣＮ（ＩＤ１）と、ＩＳＲＣのシリアル番号（ＩＤ２）と、ディスクＩＤ（ＩＤ３）とを加算したものを、ハッシュ関数によって計算して得る方法で生成されている。

【００７８】ここで、ハッシュ関数とは、所定長の文章（文章データ）を入力とし、固定長のメッセージダイジェスト（メッセージダイジェストデータ）を出力とする関数である。なお、メッセージダイジェストとは、ハッシュ値とも称されることもある。また、以下の説明では、この所定長の文章は、例えば１２８ビットのディスクＩＤ等を意味するものとし、具体的には、ディスクＩＤ等を組み合わせたものを適当な長さに分割して得られたものに相当する。そして、入力されるビット長は、１２８ビットに限らず、８０ビットにしたり、２００ビットにできる。すなわち、短い場合は暗号化処理と復号化処理との負担が軽減するが、安全性が担保されなくなる。逆に、長い場合は暗号化処理と復号化処理との負担が増大するが、安全性が担保される。すなわち、このビット長は、設計方針によって変更されうる。

【００７９】また、ＭＣＮ，ＩＳＲＣのシリアル番号，ディスクＩＤを全て加算したものが、１２８ビットに満たない場合には、ＭＣＮ，ＩＳＲＣのシリアル番号，ディスクＩＤを加算したものに、ビット列（キーメッセージ）が付加され、１２８ビットにされてから、ハッシュ関数による演算が行なわれるようになっている。さらに、キーメッセージに関しては、ソフトウェア（ドライバーソフト）が自動的に固定メッセージを挿入するようにしてもよく、あるいは、ユーザが挿入するようにしてもよい。また、記録する情報の種類に応じたキーメッセージが付加されるようにしてもよい。そして、暗号化キーの安全性を高めるために、キーメッセージは、ディスクＩＤが記録されているディスクと同一のディスクには記録されないようにする。

【００８０】従って、この暗号化は、ビット長を変化させうるキーメッセージ，ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を種とするハッシュ関数を用いて行なわれていることになり、また、この暗号化は、キーメッセージ，ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を組み合わせた情報を種とするハッシュ関数を用いて行なわれていることになる。

【００８１】次に、このＣａｓｅ３のハッシュ関数の種類について、具体的なプログラム例を用いて説明する。上述のように、ハッシュアルゴリズムは、ＭＤ方式に基づくものと、その他のものとがあり、種々提案されている。例えば、ＲＳＡ社のRonald L. Rivest氏が開発したＭＤ２（Message Digest #2），ＭＤ４（Message Digest #4），ＭＤ５（Message Digest #5）や、H. Dobbertin

23

氏が開発したＲＩＰＥＭＤ（Race Integrity Primitive Evaluation MessageDigest）や、米国ＮＩＳＴ（National Institute of Standards and Technology）によりＦＩＰＳ（Federal Information Processing Standards）のＰＵＢ１８０に定められたＳＨＡ（Secure Hash Algorithm）等がある。

【００８２】ここで、ＭＤ２は、１２８ビットのメッセージダイジェストを生成するアルゴリズムであり、ＰＥＭに使用された。そして、ＭＤ４は、ＭＤ２の処理速度が遅い点を解決するために開発されたアルゴリズムであって、ＲＦＣ１３２０（Request for Comments 1320）に規定されている。また、このＭＤ４は、１２８ビットのメッセージダイジェストを生成し、処理速度が速く、ＭＤ５よりも効率的にメッセージダイジェストを作成できる。その半面、異なる種から生成されたメッセージダイジェスト値が、同一の値を出力する、いわば値の衝突が発生することがある。

【００８３】また、ＭＤ５は、１２８ビットのメッセージダイジェストを生成するアルゴリズムであって、ＲＦＣ１３２１に規定されている。このＭＤ５は、任意長の文章を基に、固定長のメッセージダイジェストを効率よく生成することができ、電子署名に使用されることもある。すなわち、ＭＤ５は、元の文章に付する指紋のような役割をもしている。さらに、ディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号が異なったときに、同一の暗号化キーが生成される確率が、極めて小さくなる。

【００８４】これらのＭＤ方式を用いることによって、メッセージダイジェストの大きさを容易に変化させることができ、また、３２ビットあるいは６４ビットのＣＰＵを用いたソフトウェア処理が高速に行なわれる。一方、ハッシュアルゴリズムは、これらＭＤ方式の他、ＲＩＰＥＭＤやＳＨＡといったアルゴリズムを有する。このＲＩＰＥＭＤは、１６０ビットのメッセージダイジェスト

24

を生成するアルゴリズムである。また、ＳＨＡは、ＳＨＡ－１はＭＤ４を改良したアルゴリズムであり、任意長の文章からＭＤ４やＭＤ５よりも長い１６０ビット長のメッセージダイジェストを生成することができ、ＦＩＰＳ１８０－１で規定されている。

【００８５】図４０は、ハッシュ関数のプログラム例を示す図である。この図４０に示す関数ｆｕｎｃ（）は、最良のハッシュ関数（最良ハッシュ関数）のアルゴリズムを有するものであり、入力変数はポインタの（＊ｓｔｒ）であり、出力はメッセージダイジェスト（ｖａｌ％ＳＩＺＥ）である。そして、メイン関数等の他の関数（図示省略）が、この関数ｆｕｎｃ（）に所定長のビット列の先頭位置を表すポインタ（＊ｓｔｒ）を渡して、関数ｆｕｎｃ（）を呼び出す。そして、ｌｅｎ＝ｓｔｒｌｅｎ（ｓｔｒ）にて、入力された所定数のビット列の長さが求められて、ハッシュ値ｖａｌが計算される。このｖａｌは、２６進数で表された３桁の値であって、それぞれ、１０進数の１の位、１０の位、１００の位に相当する。ここで、＊ｓｔｒ－‘ａ’は、入力文字列の先頭を表すものであり、＊（ｓｔｒ＋ｌｅｎ／２）－‘ａ’は、入力文字列の中央部を表すものであり、さらに、＊（ｓｔｒ＋（ｌｅｎ－１））－‘ａ’は、入力文字列の最後尾を表すものである。そして、この出力されたｖａｌは、ＳＩＺＥ（例えば１０２３）で除算されて、１０２３種類の剰余に分類されるのである。これにより、入力されたアルファベット列の全てが、１０２３種類のメッセージダイジェストに置換される。なお、ポインタ変数が０（ＮＵＬＬ）の場合は、ハッシュアルゴリズムの演算は行なわれずに、０が出力されるようになっている。

【００８６】

【表１】

ハッシュ関数を用いた計算の実行条件の一例

サイズ：1023
繰り返し回数：10

データ総数(個)	挿入時間(秒)	検索時間(秒)	削除時間(秒)	要素数の平均	要素数の最大値	要素数の最小値
50000	1.5850	2.6950	1.6550	35.266	54.400	23.000

【００８７】

【表２】

25　　26

ハッシュ関数により生成されたデータの分布の一例

ハッシュ値の範囲	生成されたデータ個数(1つの＊は50の要素数に相当)	
table[0 ～ 49]:	**********	1922
table[50 ～ 99]:	**********	1930
table[100 ～ 149]:	**********	1904
table[150 ～ 199]:	**********	1968
table[200 ～ 249]:	**********	1765
table[250 ～ 299]:	**********	1834
table[300 ～ 349]:	**********	1836
table[350 ～ 399]:	**********	1781
table[400 ～ 449]:	**********	1749
table[450 ～ 499]:	**********	1876
table[500 ～ 549]:	**********	1707
table[550 ～ 599]:	**********	1747
table[600 ～ 649]:	**********	1756
table[650 ～ 699]:	**********	1738
table[700 ～ 749]:	**********	1806
table[750 ～ 799]:	**********	1768
table[800 ～ 849]:	**********	1753
table[850 ～ 899]:	**********	1840
table[900 ～ 949]:	**********	1778
table[950 ～ 999]:	**********	1806
table[1000 ～ 1022]:	**********	850

ヒストグラム平均:1813.978495
平均:36.279570
最大値:57
最小値:21

【００８８】表１はハッシュ関数を用いた計算の実行条件を示す表であり、この表１に示すように、入力されるデータ数（データ総数）は５００００個であり、また、１０回繰り返したものである。さらに、表２はハッシュ関数により生成されたデータの分布の一例を示す表であって、ｔａｂｌｅはメッセージダイジェスト値（ハッシュ値）の範囲を表し、＊はその範囲のヒストグラム（生成されたデータ個数）を表す。ここで、１つの＊に含まれる要素数は５０である。例えば、この表２のｔａｂｌｅ[０～４９]と記されたところの右側に、＊で量を表すヒストグラムが描かれており、その右側に１９２２と付されているものは、メッセージダイジェストの値であって、０から４９までの値を示すものが１９２２個生成されたことを示している。従って、このヒストグラムから、ほぼ同一の頻度でメッセージダイジェストが生成されていることがわかる。

【００８９】なお、図３９，図４０及び表１，表２に示した乱数関数Ｒｎｄ（）やハッシュ関数Ｈａｓｈ（）を用いた暗号化キー生成方法は、後述する第２実施形態、第３実施形態及び各変形例においても、同様に用いられる。さらに、上記のプログラム例においては、２バイト処理を行なうようにすれば、入力文章として日本語を使用することも可能である。

【００９０】このように、ハッシュ関数Ｈａｓｈ（）を用いることによって、同一結果が出力されるようになり、かつ、逆解析がされにくい暗号化キーが生成されるようになる。すなわち、これら詳述した乱数関数Ｒｎｄ（）やハッシュ関数Ｈａｓｈ（）を使用することによって、同一のディスクＩＤからは同一の暗号化キーが生成される。加えて、これらの関数は、逆関数をもたないので、生成された暗号化キーから元のディスクＩＤ等を復元するのが困難であり、秘匿性が高まる。

【００９１】また、秘匿性に関しては、通常のユーザレベルにおいて、パソコンを用いて解読する場合、そのパソコンに搭載されているＣＰＵのバスラインの数やメモリのビット数等では、１２８ビットのメッセージダイジェストを解読することは、不可能に近い。従って、ユーザは、音楽，映画，コンピュータプログラム等の著作権付きのデータを、実際上は、二次コピーできず、この著作権付きデータが保護されるのである。

【００９２】このように、ユーザのドライブ装置でも読み取り可能なＰＭＡと、データ領域１２ｂに分散されて記録されたＭＣＮ，ＩＳＲＣとによって、暗号化のために必要なビット数が確保されるようになっている。図７は、本発明の第１実施形態に係る暗号化キー刷り込み装置の模式図である。この図７に示す暗号化キー刷り込み

装置１９は、音声、映像、データ等のマルチメディアデータを暗号化して暗号化データとして記録するものであって、パソコン２０と、ケーブル４３と、ＣＤ－Ｒ／ＲＷドライブ４６とをそなえて構成されている。また、ＣＤ－Ｒディスク（ＣＤ－Ｒメディア）４７ａ又はＣＤ－ＲＷディスク（ＣＤ－ＲＷメディア）４７ｂは、初期化前のディスク（メディア）である。

【００９３】このパソコン２０は、ＣＤ－Ｒディスク４７ａ又はＣＤ－ＲＷディスク４７ｂの初期化を行なうものであって、メディア番号設定手段４５をそなえて構成されている。このメディア番号設定手段４５は、ＭＣＮ，ＩＳＲＣのシリアル番号の値を設定するものであり、操作する者が入力した値を一時的に保管できるように、Mode Select コマンド用メモリ（図示せず）を有する。また、このパソコン２０は、ディスクの初期化の際に、論理フォーマットであるＵＤＦ(Universal Disk Format）を施すようになっている。

【００９４】このパソコン２０は、ユーザがコピーする際に、ユーザが使用するソフトウェア（例えば、Direct CD;Adaptec社の商品名）に対応した論理フォーマットを実行できるようになっている。ここで、DirectCDとは、ユーザがコピーする際に、ＣＤ－Ｒ／ＲＷドライブ４６に入っているファイルを、内蔵ディスクやフロッピーディスクに入っているファイルを扱うのと同様な環境で取り扱いができるようにした書き込み用のソフトウェアである。

【００９５】そして、ディスクを初期化する際には、ユーザが、DirectCDを用いて論理フォーマットを行なう。また、ユーザがISO9660 との互換を取りたい場合は、ISO9660 の論理フォーマットをも加えることができ、その場合、ISO9660 とDirectCDとの併せて２種類のフォーマットを行なう必要がある。このISO9660(Internatinal Organization for Standardization 9660) は、国際規格であり、ＣＤ－ＲＯＭ又は、ＣＤ－Ｒ／ＲＷにおけるファイル、ディレクトリ構造及び論理フォーマット等が定義されている。また、ISO9660 は拡張可能な仕様になっており、様々な拡張仕様が規定されている。さらに、ISO9660 は、情報交換水準があり、レベル１からレベル３まで定義されている。なお、一般には、ISO9660 ではレベル１を指す。これは、使用できる文字や、ファイル名の使用の規格が入っている。

【００９６】なお、このパソコン２０は、その他の公知の機能を有するが、その詳細な説明を省略する。そして、ケーブル４３は、パソコン２０とＣＤ－Ｒ／ＲＷドライブ４６とを電気的に接続するものである。また、ＣＤ－Ｒ／ＲＷドライブ４６は、挿入されたディスクに上記のディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号を記録するものである。

【００９７】これにより、暗号化キー刷り込み装置１９内のパソコン２０のメディア番号設定手段４５において、ＭＣＮ，ＩＳＲＣのシリアル番号が設定され、その設定された値が、ケーブル４３を介して、ＣＤ－Ｒ／ＲＷドライブ４６に入力される。そして、このＣＤ－Ｒ／ＲＷドライブ４６において、ＭＣＮ，ＩＳＲＣのシリアル番号が記録されるとともに、自動的にディスクＩＤが記録されるのである。

【００９８】このような構成によって、ＣＤ－Ｒ／ＲＷのコピー防止のための、初期化が行なわれる。図８から図１１を用いて、ＣＤ－ＲＷとＣＤ－Ｒとの初期化フローを説明する。図８は、本発明の第１実施形態に係る、ＣＤ－ＲＷのコピー防止方法における初期化フローチャートである。

【００９９】本発明の記録媒体の初期化方法は、ドライブ装置（図示省略）が読み出し可能な領域であってユーザはその領域をアクセスできない管理領域１１と、ドライブ装置が読み出し可能な領域であってユーザがその領域を任意にアクセスできるデータ領域１２ｂとをそなえた記録媒体（ディスク１０）の初期化方法であって、その管理領域１１に暗号化のためのディスクＩＤを記録するものである。

【０１００】ステップＡ１から開始される初期化ステップは、まず、ステップＡ２において、ＣＤ－ＲＷディスク（ＣＤ－ＲＷメディア）４７ｂがＣＤ－Ｒ／ＲＷドライブ４６に挿入される。そして、ステップＡ３において、Mode Select コマンド用メモリ（図示せず）が確保され、さらに、ステップＡ４において、暗号化キー１が、 Select コマンド用メモリに設定され、ステップＡ５において、暗号化キー２が、 Select コマンド用メモリに設定される。そして、ステップＡ６において、Mode Select コマンドが発行されることにより、これらの暗号化キー１，暗号化キー２とが用意されるのである。

【０１０１】ここで、ステップＡ７において、Formatコマンドが発行され、暗号化キー１と暗号化キー２とが、実際にデータ領域１２ｂに書き込まれ、また、暗号化キー３が管理領域１１に書き込まれるのである。すなわち、データ領域１２ｂに、Ｑチャネルサブコードのモード２形式でＭＣＮが記録され（第２書込ステップ）、Ｑチャネルサブコードのモード３形式でＩＳＲＣのシリアル番号が記録される（第３書込ステップ）。

【０１０２】なお、この暗号化キー３は、ＣＤ－Ｒ／ＲＷドライブ４６によって、自動的に発行され、上記の管理領域１１に暗号化のためのディスクＩＤが記録されるのである（第１書込ステップ）。そして、このステップＡ７で、暗号化キーの刷り込みが終了する。従って、本発明の記録媒体初期化方法は、上記のディスクＩＤを記録するに当たり、管理領域１１に暗号化のためのディスクＩＤを記録する第１書込ステップと、データ領域１２ｂにＱチャネルサブコードのモード２形式でディスクＩＤ，ＭＣＮ（媒体識別番号情報）を記録する第２書込ステップと、データ領域１２ｂにＱチャネルサブコードの

モード３形式でＩＳＲＣのシリアル番号（シリアル番号情報）を記録する第３書込ステップとをそなえて構成されたことになる。

【０１０３】次に、Write コマンド用メモリが確保され（ステップＡ８）、DirectCD用の論理フォーマットのデータが、Write コマンド用メモリに設定される（ステップＡ９）。さらに、ステップＡ１０において、Write コマンドが発行されて、論理フォーマットデータが記録される。なお、このステップＡ１０は、概ね、リードインの直後である。そして、最後に、ＣＤ－ＲＷディスク（ＣＤ－ＲＷメディア）４７ｂがＣＤ－Ｒ／ＲＷドライブ４６から、排出され（ステップＡ１１）、初期化ステップが終了する（ステップＡ１２）。

【０１０４】これにより、１セッションへの書き込みが終了するが、複数のセッションに跨がって書き込まれる場合は、この後、以上のステップが複数回繰り返される。そして、このようにして、論理フォーマットが行なわれた後、次のセッションより、ユーザは、データを記録できるようになる。図９，図１０，図１１はいずれも、本発明の第１実施形態に係る、ＣＤ－Ｒのコピー防止方法における初期化フローチャートであり、セッション１（ＳＥＳＳＩＯＮ１）とセッション２（ＳＥＳＳＩＯＮ２）との２つのセッションが書き込まれる例を表している。また、これらの図９，図１０，図１１に示すフローチャートは、図８と比較して、２種類の論理フォーマットデータが書き込まれる点が異なっている。なお、このフローも上記の図７に示す暗号化キー刷り込み装置１９を用いて実行される。

【０１０５】また、図９，図１０，図１１のフローチャートに従って、記録が行なわれた後のＣＤ－Ｒディスク４７ａ（又はＣＤ－ＲＷディスク４７ｂ）上でのデータレイアウトは図１２のようになる。図１２は、本発明の第１実施形態に係る初期化後のＣＤ－Ｒ／ＲＷのデータレイアウトを示す図である。この図１２に示すＣＤ－Ｒディスク４７ａ（又はＣＤ－ＲＷディスク４７ｂ）上のトラック１は、ISO9660 用の論理フォーマットデータであり、トラック２は、DirectCD用の論理フォーマットデータである。そして、後述するように、トラック２が書き込まれた後に、トラック１が書き込まれる。

【０１０６】ステップＢ１（図９参照）から開始される初期化ステップは、まず、ステップＢ２において、ＣＤ－Ｒディスク（ＣＤ－Ｒメディア）４７ａがＣＤ－Ｒ／ＲＷドライブ４６に挿入され、ステップＢ３において、セッション１の書き込みが開始される。すなわち、上述したものと同様に、Mode Select コマンド用メモリ（図示せず）が確保され（ステップＢ４）、ステップＢ５において、暗号化キー１が、 Select コマンド用メモリに設定され、ステップＢ６において、暗号化キー２が、 Select コマンド用メモリに設定される。さらに、ステップＢ７において、Mode Select コマンドが発行されることにより、これらの暗号化キー１，暗号化キー２とが、設定されるのである（第２書込ステップ，第３書込ステップ）。

【０１０７】次に、ステップＢ８において、ISO9660 の論理フォーマット領域として後で使用するために、Reserve Track コマンドの発行がされ、ISO9660 の論理フォーマットのためのトラック１（図１２参照）が確保される。そして、トラック１が確保された後に、①と付したステップ（ステップＢ９～ステップＢ１１）において、DirectCDの論理フォーマットデータがトラック２（図１２参照）に書き込まれる。すなわち、Write コマンド用メモリが確保され（ステップＢ９）、DirectCD用の論理フォーマットデータが、Write コマンド用メモリに設定され（ステップＢ１０）、ステップＢ１１において、Write コマンドが発行されて、実際に論理フォーマットデータが記録される。従って、③と付したステップは、①と付したステップのために行なわれている。そして、図９に示すＡと付した箇所に続いて、図１０の最上部のＡと付した箇所から始まるISO9660 の論理フォーマットデータの書き込みが行なわれる。

【０１０８】すなわち、同様に、Mode Select コマンド用メモリ（図示せず）が確保され（ステップＢ１２）、暗号化キー１が Select コマンド用メモリに設定され（ステップＢ１３）、暗号化キー２が Select コマンド用メモリに設定され（ステップＢ１４）、さらに、ステップＢ１５において、Mode Select コマンドが発行されることにより、これらの暗号化キー１，暗号化キー２とが、設定される（第２書込ステップ，第３書込ステップ）。

【０１０９】次に、ISO9660 の論理フォーマットデータの書き込みが、②と付したステップ（ステップＢ１６～ステップＢ１８）で行なわれ、上記のステップＢ８にて確保されたトラック１に、ISO9660 の論理フォーマットが行なわれるのである。すなわち、Write コマンド用メモリが確保され（ステップＢ１６）、ISO9660用の論理フォーマットデータが、Write コマンド用メモリに設定される（ステップＢ１７）。さらに、ステップＢ１８において、Write コマンドが発行されて、論理フォーマットデータが記録される。従って、④と付したステップは、②と付したステップのために行なわれている。また、ステップＢ１９において、CloseSession コマンドが発行されて、図１２に示すようなリードイン１とリードアウト１とが書き込まれ、セッション１の書き込みが終了する（ステップＢ２０）。

【０１１０】このセッション１が終了すると、通常のドライブ装置でセッション１を読めるようになり、セッション２以降にデータを記録する際に、セッション１に記録された暗号化キーを利用して、暗号化を行なうことができる。そして、図１０に示すＢと付した箇所に続いて、図１１の最上部のＢと付した箇所から始まるセッシ

ョン２の書き込みが開始されるのである。

【０１１１】また、トラック１での暗号化キーは、トラック２での暗号化キーと、同一であっても異なっていてもよい。これにより、操作者は、複数の暗号化キー１及び暗号化キー２を別々に設定できる場合があり、その場合は、トラック毎に、個別に暗号化キーを設定できる。ステップＢ２１から始まるセッション２では、まず、Reserve Track コマンドの発行がされ（ステップＢ２２）、Write コマンド用メモリが確保され（ステップＢ２３）、論理フォーマットデータが、Write コマンド用メモリに設定され（ステップＢ２４）、さらに、ステップＢ２５において、Write コマンドが発行されて、論理フォーマットデータが記録される。そして、最後に、ＣＤ－Ｒディスク（ＣＤ－Ｒメディア）４７ａがＣＤ－Ｒ／ＲＷドライブ４６から、排出され（ステップＢ２６）、初期化ステップが終了する（ステップＢ２７）。

【０１１２】セッション２での暗号化キーは、セッション１と同一であっても、異なっていてもよい。これにより、操作者は、複数の暗号化キー１，暗号化キー２を、別々に設定できる場合があり、その場合は、個別な暗号化キーを設定できる。そして、この初期化ステップの後に、初期化されたディスク（ＣＤ－Ｒディスク４７ａ又はＣＤ－ＲＷディスク４７ｂ）を用いて、ユーザが１回目のコピーをするときは、読み込まれた音声，映像，データ等のマルチメディアデータは、ディスク（メディア）固有の暗号化キーにより、暗号化されて、ユーザは、１枚の特定ディスクを得られるが、ユーザが、その特定ディスクから、他のディスクへコピーをしても、その特定ディスクに格納されている暗号化データを復号するために必要なメディア番号（ディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号）が異なるので、元の音楽や映像データが復元されることはない。

【０１１３】このようにして、音楽や映画等の著作権付きのデータが、１枚のディスクに１回だけコピーできるが、そのコピーされたディスクから他のディスクへ二次コピーすることはできないので、著作権付きのデータが保護される利点がある。そして、このようにして、録音・再生機器に、使用料を予め上乗せしたりせずに、著作権付きデータの保護が図れる利点がある。

【０１１４】さらに、既存の領域に暗号化キーとなるデータを分散して記録し、その分散されて記録されたデータを寄せ集めて暗号化キーを生成しているので、ディスクのフォーマット方法を変更しなくても、暗号化が行なえる利点がある。また、ディスク内での分散方法は、必要に応じて、種々に変更させることができるので、暗号化キーとして秘匿性を保持し、その強度を高められる利点がある。

【０１１５】加えて、暗号化キーの生成は、乱数関数Ｒｎｄ（）やハッシュ関数Ｈａｓｈ（）を用いてなされるので、同一のディスクＩＤ等からは同一の暗号化キーが

得られるとともに、出力された暗号化キーから元のディスクＩＤ等は解読されなくなる。従って、暗号化キーに関して秘匿性が高まり、著作権付きのデータの二次コピーが防止されるようになる。

（Ａ１）第１実施形態の第１変形例の説明

上記の暗号化キー刷り込み装置１９を、他の装置に組み込んで別態様の暗号化方法が行なえる。以下、第１実施形態の第１変形例から第３変形例として、それらの例を説明する。

【０１１６】図１３は、本発明の第１実施形態の第１変形例に係る暗号化・復号化キー記録装置の模式図である。この図１３に示す暗号化・復号化記録装置４０は、インターネットサーバ２３と回線３６を介して接続されている。この暗号化・復号化記録装置４０は、初期化されたＣＤ－Ｒディスク又はＣＤ－ＲＷディスクに、音声、映像、データ等のマルチメディアデータを暗号化して暗号化データとして記録する暗号化装置であるとともに、その暗号化データを復号する復号化装置であって、パソコン２０と、ケーブル４３と、ＣＤ－Ｒ／ＲＷドライブ２２とをそなえて構成されている。

【０１１７】また、暗号化キーの生成方法に関しては、第１実施形態にて説明（図３９～図４０参照）したのと同様に、３種類の態様がある。すなわち、暗号化が、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を個別に用いて行なわれたり、又は、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を組み合わせた情報を用いて行なわれるようにしてもよい。さらに、暗号化が、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を種とする乱数関数を用いてもよく、又は、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を組み合わせた情報を種とする乱数関数を用いて行なうようにもできる。加えて、暗号化が、キーメッセージ，ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を種とするハッシュ関数を用いてもよく、又は、キーメッセージ，ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を組み合わせた情報を種とするハッシュ関数を用いて行なうようにもできる。

【０１１８】また、ＣＤ－Ｒ／ＲＷドライブ２２に挿入されるディスクは、初期化されたＣＤ－Ｒディスク２１ａ，ＣＤ－ＲＷディスク２１ｂ又は、データが記録されたＣＤ－Ｒディスク３１ａ，ＣＤ－ＲＷディスク３１ｂである。さらに、これらの管理領域１１（図１参照）には、暗号化のためのディスクＩＤが刷り込まれている（記録されている）。なお、以下の各実施形態及びその変形例での説明において、初期化されたＣＤ－Ｒディスク２１ａ又はＣＤ－ＲＷディスク２１ｂを書き込み用ディスクと称することがある。また、同様に、データが記録されたＣＤ－Ｒディスク３１ａ又はＣＤ－ＲＷディスク３１ｂを再生用ディスクと称することがある。さらに、ＣＤ－Ｒディスク２１ａ，ＣＤ－ＲＷディスク２１

ｂ，ＣＤ－Ｒディスク３１ａ，ＣＤ－ＲＷディスク３１ｂをまとめて、ディスクと称することがある。

【０１１９】このパソコン２０は、復号化手段２０ｃと、第２暗号鍵生成手段２０ｄとをそなえて構成されている。この復号化手段２０ｃは、暗号化された情報を暗号化キーを用いて復号し、音声、映像、データ等の情報を含むマルチメディアデータを再生しうるものであり、第２暗号鍵生成手段２０ｄは、ディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号から暗号化キーを生成するものである。これらの機能は、例えばソフトウェアによって、発揮される。なお、パソコン２０のその他の機能の説明を省略する。

【０１２０】また、ＣＤ－Ｒ／ＲＷドライブ２２は、ＣＤ－Ｒディスク２１ａ又はＣＤ－ＲＷディスク２１ｂを読み取り又は書き込みしうるものであって、読出手段２２ａと、暗号化メディア情報保存手段２２ｂと、第２読出手段２２ｃとをそなえて構成されている。ここで、読出手段２２ａは、書き込み用ディスク及び再生用ディスクにおけるディスクＩＤを読み出しうるものである。また、書き込み用ディスクは、図１に示すディスク１０と同様、ＣＤ－Ｒ／ＲＷドライブ２２が読み出し可能な領域であってユーザはその領域をアクセスできない管理領域１１と、ＣＤ－Ｒ／ＲＷドライブ２２が読み出し可能な領域であってユーザがその領域を任意にアクセスできるデータ領域１２ｂとをそなえ、管理領域１１に暗号化のためのディスクＩＤが記録されている。

【０１２１】また、暗号化メディア情報保存手段２２ｂは、暗号化データを、同一のディスクＩＤを有する書き込み用ディスクのデータ領域１２ｂに保存しうるものであり、また、第２読出手段２２ｃは、書き込み用ディスク及び再生用ディスクにおけるディスクＩＤを読み出しうるものである。また、この書き込み用ディスク及び再生用ディスクは、図１に示すディスク１０と同様、ＣＤ－Ｒ／ＲＷドライブ２２が読み出し可能な領域であってユーザはその領域をアクセスできない管理領域１１と、ＣＤ－Ｒ／ＲＷドライブ２２が読み出し可能な領域であってユーザがその領域を任意にアクセスできるデータ領域１２ｂとをそなえ、管理領域１１に暗号化のためのディスクＩＤが記録されるとともに、データ領域１２ｂに暗号化された情報が記録されている。

【０１２２】そして、これらの機能は、それぞれ、ＣＤ－Ｒ／ＲＷドライブ２２内のドライブ装置（図示せず）によって発揮される。なお、ＣＤ－Ｒ／ＲＷドライブ２２のその他の機能についての詳細な説明を省略する。さらに、インターネットサーバ２３は、インターネット上で音声，映像，データ等のマルチメディアデータを、暗号化して転送するものであって、暗号化メディア情報生成手段２３ａと、暗号鍵生成手段２３ｂとをそなえて構成されている。この暗号化メディア情報生成手段２３ａは、上述の暗号化メディア情報生成手段２０ａと同一のものであり、その詳細な説明を省略する。また、暗号鍵生成手段２３ｂは、ディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号から暗号化キーを生成しうるものである。

【０１２３】また、回線３６は、このインターネットサーバ２３と暗号化・復号化記録装置４０とを接続する回線であり、例えばローカルエリアネットワークにより、この回線機能は、発揮される。なお、ケーブル４３は、上述したものと同一であるので、その説明を省略する。これにより、暗号化・復号化記録装置４０においては、ＣＤ－Ｒ／ＲＷドライブ２２内の読出手段２２ａにおいて、挿入された書き込み用ディスクのディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号がメディア番号として読み出される（第１ディスク識別情報読出ステップ）。その読み出されたメディア番号は、ケーブル４３を介して、パソコン２０に入力された後、そのメディア番号は、インターネットサーバ２３に、回線３６を介して、送信され、インターネットサーバ２３内の暗号鍵生成手段２３ｂにおいて、そのディスクＩＤとＭＣＮとの組み合わせ、ディスクＩＤとＩＳＲＣのシリアル番号との組み合わせ、又は、ディスクＩＤとＭＣＮとＩＳＲＣのシリアル番号との組み合わせで、暗号化キーが生成される（第１暗号鍵生成ステップ）。

【０１２４】そして、インターネットサーバ２３内の暗号化メディア情報生成手段２３ａにおいて、音声、映像、データ等のマルチメディアデータが、読み出され（第１読出ステップ）、上記のメディア番号を用いた暗号化キーによって暗号化されて暗号化データが出力される。さらに、この暗号化データは、回線３６を介して、暗号化・復号化記録装置４０内のＣＤ－Ｒ／ＲＷドライブ２２に入力され、ＣＤ－Ｒ／ＲＷドライブ２２内の暗号化メディア情報保存手段２２ｂによって、その暗号化キーを用いて暗号化データが生成され、送信されたディスクＩＤを有するディスクのデータ領域１２ｂ（図１参照）に記録されることにより、特定ディスクが生成されるのである（特定記録媒体生成ステップ）。

【０１２５】一方、復号は、次のように行なわれる。すなわち、書き込み用ディスク又は、再生用ディスクが、ＣＤ－Ｒ／ＲＷドライブ２２に挿入され、ＣＤ－Ｒ／ＲＷドライブ２２内の第２読出手段２２ｃにおいて、そのディスクのディスクＩＤ、ＭＣＮ、ＩＳＲＣが読み出され、これらのディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号は、ケーブル４３を介して、パソコン２０に入力される。同様に、その書き込み用ディスク又は、再生用ディスクから暗号化データが読み出される。

【０１２６】また、パソコン２０内の第２暗号鍵生成手段２０ｄにおいて、そのディスクＩＤとＭＣＮとの組み合わせ、ディスクＩＤとＩＳＲＣのシリアル番号との組み合わせ、又は、ディスクＩＤとＭＣＮとＩＳＲＣのシリアル番号との組み合わせから暗号化キーが生成される。そして、パソコン２０内の復号化手段２０ｃにおい

35

て、その暗号化キーが、送信した暗号化キーと一致する場合のみ、暗号化データが復号されて再現され、書き込み用ディスク又は、再生用ディスクの暗号化データが暗号化キーを用いて復号されるのである。

【０１２７】このような構成によって、ＣＤ－Ｒ／ＲＷのコピー防止のための、暗号化及び復号化が行なわれる。まず、第１実施形態にて説明した初期化ステップによって、暗号化キーが書き込み用ディスクに刷り込まれ、その後に、その初期化された書き込み用ディスクに、実際に音楽データが記録される。図１４は、本発明の第１実施形態の第１変形例に係る、ＣＤ－Ｒ又はＣＤ－ＲＷのコピー防止方法のフローチャートである。

【０１２８】ステップＣ１から開始されるコピー防止ステップは、まず、ユーザは、インターネットのサイトに接続し（ステップＣ２）、ステップＣ３において、暗号化・復号化記録装置４０からインターネットサーバ２３に対して、そのディスクのメディア番号（ディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号）が送信される。なお、このステップＣ３までは、データの状態は、通常のものである。

【０１２９】次に、ステップＣ４において、インターネットサーバ２３は、ディスク（メディア）固有の暗号化キーであるメディア番号（ディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号）によって、その送信されたデータを暗号化する。続いて、ステップＣ５において、その暗号化データが、インターネットサーバ２３から暗号化・復号化記録装置４０に対して、転送される。さらに、ステップＣ６において、その転送されたデータは、パソコン２０によって、処理されて、書き込み用ディスクに保存される。

【０１３０】一方、復号ステップとして、ステップＣ７で、そのディスク（メディア）固有の暗号化キーによって、そのデータが復号され、ステップＣ８で、その元のデータが再生されて、ステップＣ９で、復号ステップが終了するのである。ここで、ステップＣ６，Ｃ７，Ｃ８においては、ステップＣ３で送信された暗号化キー以外の暗号化キーで復号することはできない。

【０１３１】換言すれば、暗号化キーとして使用したディスク以外のディスクに書き込まれた場合には、データを復元することはできない。すなわち、メディア番号が一致しないと、そのメディア番号から暗号化キーを生成して暗号化データを復号しても、元のデータを再現することはできない。このようにして、暗号化キーが刷り込まれた１枚の特定ディスクが得られ、この特定ディスクから、他のディスクへコピーをしようとしても、その特定ディスクに格納されている暗号化データを復号するために必要なメディア番号（ディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号）が異なるので、元のデータが復元されることはない。さらに、暗号化キーを直接インターネット上で送信するのでなく、ディスクＩＤ，ＭＣＮ，

36

ＩＳＲＣのシリアル番号を送信するようになっているので、暗号化キーを他人に盗まれるおそれがない。

【０１３２】また、このようにして、音楽や映画等の著作権付きのデータが、１枚のディスクに１回だけコピーできるが、そのコピーされたディスクから他のディスクへ二次コピーすることはできないので、著作権付きのデータが保護される。そして、このようにして、録音・再生機器に、使用料を予め上乗せしたりせずに、著作権付きデータの保護が図れる利点がある。

【０１３３】さらに、暗号化キーの記録の際は、既存の領域に暗号化キーとなるデータが分散されて記録され、その分散して記録されたデータが寄せ集められて暗号化キーが生成されるので、ディスクのフォーマット方法の変更なしに、暗号化が行なえる利点がある。また、ディスク内での分散方法は、必要に応じて、種々に変更が可能なので、暗号化キーとしての秘匿性は保持され、その強度が高められる利点がある。

【０１３４】そして、暗号化キーの生成は、乱数関数Ｒｎｄ（）やハッシュ関数Ｈａｓｈ（）を用いてなされるので、同一のディスクＩＤ等からは同一の暗号化キーが得られるとともに、出力された暗号化キーから元のディスクＩＤ等は解読されなくなる。従って、暗号化キーに関して秘匿性が高まり、著作権付きのデータの二次コピーが防止されるようになる。

（Ａ２）第１実施形態の第２変形例の説明

音楽ＣＤからデータを読み出すような態様でも可能である。

【０１３５】図１５は、本発明の第１実施形態の第２変形例に係る暗号化・復号化記録装置の模式図である。この図１５に示す暗号化・復号化記録装置４０ａは、パソコン２０と、ＣＤ－Ｒ／ＲＷドライブ２２とをそなえるほか、ＣＤドライブ２４と、ケーブル４３ａ，４３ｂとをそなえて構成されている。また、ＣＤメディア２５は、音楽データが入ったものであって、いわゆる音楽用ＣＤと呼ばれるものであり、そして、ＣＤ－Ｒ／ＲＷドライブ２２には、書き込み用ディスク（ＣＤ－Ｒディスク２１ａ，ＣＤ－ＲＷディスク２１ｂ）または、再生用ディスク（ＣＤ－Ｒディスク３１ａ，ＣＤ－ＲＷディスク３１ｂ）が挿入されるようになっている。さらに、この図１５に示すＣＤドライブ２４は、ＣＤメディア２５を読み出して再生するものであり、複数のＣＤメディア２５を選択できるようになっている。

【０１３６】また、ケーブル４３ａは、パソコン２０とＣＤドライブ２４とを電気的に接続するものであり、さらに、ケーブル４３ｂは、ＣＤドライブ２４とＣＤ－Ｒ／ＲＷドライブ２２とを電気的に接続するものであり、これによって、パソコン２０とＣＤ－Ｒ／ＲＷドライブ２２との間で、データ及び暗号化データが、送受できるようになっている。

【０１３７】なお、パソコン２０は、暗号化メディア情

37

報生成手段２０ａ，暗号鍵生成手段２０ｂ，復号化手段２０ｃ，第２暗号鍵生成手段２０ｄをそなえて構成されている。ここで、暗号化メディア情報生成手段２０ａは、ディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号を用いた暗号化キーによってマルチメディアデータを暗号化して暗号化データを出力しうるものである。また、暗号鍵生成手段２０ｂは、ディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号から暗号化キーを生成するものである。

【０１３８】また、暗号化キーの生成方法に関しては、第１実施形態にて説明（図３９～図４０参照）したのと同様に、３種類の態様がある。すなわち、暗号化が、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を個別に用いて行なわれたり、又は、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を組み合わせた情報を用いて行なわれるようにしてもよい。さらに、暗号化が、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を種とする乱数関数を用いてもよく、又は、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を組み合わせた情報を種とする乱数関数を用いて行なうようにもできる。加えて、暗号化が、キーメッセージ，ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を種とするハッシュ関数を用いてもよく、又は、キーメッセージ，ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を組み合わせた情報を種とするハッシュ関数を用いて行なうようにもできる。

【０１３９】さらに、復号化手段２０ｃは、暗号化データを暗号化キーを用いて復号し、音声、映像、データ等の情報を含むマルチメディアデータを再生しうるものであり、第２暗号鍵生成手段２０ｄは、ディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号から暗号化キーを生成するものである。これらは、上述したものと同一なものなので、その詳細な説明を省略する。

【０１４０】また、ＣＤ－Ｒ／ＲＷドライブ２２は、第１実施形態の第１変形例で説明したものと同一のものなので、更なる説明を省略する。これにより、暗号化は次のようになる。すなわち、ＣＤ－Ｒ／ＲＷドライブ２２内の読出手段２２ａにおいて、挿入された書き込み用ディスクのディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号がメディア番号として読み出され（第１ディスク識別情報読出ステップ）、その読み出されたメディア番号は、ケーブル４３ｂ，４３ａを介して、パソコン２０に入力される。そして、パソコン２０内の暗号鍵生成手段２０ｂにおいて、暗号化キーが生成される（第１暗号鍵生成ステップ）。

【０１４１】一方、ＣＤメディア２５に記録された、例えば音楽データは、ＣＤドライブ２４において、読み出され（第１読出ステップ）、そのデータは、ケーブル４３ａを介して、パソコン２０に入力される。そして、パソコン２０内の暗号化メディア情報生成手段２０ａにお

38

いて、その暗号化キーを用いて、その読み出されたデータは暗号化され、その暗号化データは、ケーブル４３ａ，４３ｂを介して、ＣＤ－Ｒ／ＲＷドライブ２２に入力されて、暗号化メディア情報保存手段２２ｂにおいて、暗号化データは、暗号化する際に読み出されたディスクＩＤを有する書き込み用ディスクのデータ領域１２ｂ（図１参照）に、記録することにより、特定ディスクが生成される（特定記録媒体生成ステップ）。

【０１４２】また、データを復号するときは、次のようになる。すなわち、書き込み用ディスク又は、再生用ディスクが、ＣＤ－Ｒ／ＲＷドライブ２２に挿入される。そして、ＣＤ－Ｒ／ＲＷドライブ２２内の第２読出手段２２ｃにおいて、そのディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号が読み出され、これらは、ケーブル４３ｂ，４３ａを介して、パソコン２０へと入力される。さらに、パソコン２０内の第２暗号鍵生成手段２０ｄにおいて、読み出したディスクＩＤと、ＭＣＮ，ＩＳＲＣのシリアル番号とから、暗号化キーが生成される。また、パソコン２０内の復号化手段２０ｃにおいて、書き込み用ディスク又は、再生用ディスクから読み出された暗号化データは、その暗号化キーが暗号化に使用した暗号化キーと一致する場合のみ復号され、マルチメディアデータが再現されるのである。

【０１４３】このような構成によって、ＣＤ－Ｒ／ＲＷのコピー防止のための、暗号化及び復号化が行なわれる。図１６は、本発明の第１実施形態の第２変形例に係る、ＣＤ－Ｒ又はＣＤ－ＲＷのコピー防止方法のフローチャートである。ステップＤ１から開始されるコピー防止ステップは、まず、ＣＤドライブ２４において、ＣＤメディア２５から、必要なデータが選択された後（ステップＤ２）、そのデータが読み出される（ステップＤ３）。なお、このステップまでは、データの状態は、通常のものである。

【０１４４】そして、ステップＤ４において、ＭＣＮ，ＩＳＲＣのシリアル番号，ディスクＩＤを適当に組み合わせた、そのディスク（メディア）固有の暗号化キーによって、そのデータが暗号化され、ステップＤ５において、その暗号化データが書き込み用ディスク（ＣＤ－Ｒ／ＲＷメディア）に保存される。一方、復号ステップとして、ステップＤ６で、そのディスク（メディア）固有の暗号化キーによって、そのデータが復号され、ステップＤ７で、その復号化データが使用され、ステップＤ８で、復号ステップが終了するのである。

【０１４５】また、ステップＤ４において、読み出されたデータが暗号化された後、さらに、別のデータを読み出して暗号化するようにもでき、その場合は、ディスク（図１６ではＣＤと表記されている）が入れ換えられて、ステップＤ２からステップＤ４までのステップが、繰り返される。なお、ステップＤ５，Ｄ６において、暗号化データが、暗号化キーとして使用したディスク以外

39

のディスクに書き込まれた場合には、データを復元することはできない。

【０１４６】このように、ユーザが１回目のコピーをするときは、読み込まれた音声，映像，データ等のマルチメディアデータは、ディスク固有の暗号化キーにより、暗号化されて、ユーザは、１枚の特定ディスクを得られる。逆に、ユーザが、その特定ディスクから、他のディスクへコピーをしようとしても、その特定ディスクに格納されている暗号化データを復号するために必要なメディア番号（ディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号）が異なるので、元の音楽や映像データが復元されることはない。

【０１４７】また、このようにして、音楽や映画等の著作権付きのデータが、１枚のディスクに１回だけコピーできるが、そのコピーされたディスクから他のディスクへ二次コピーすることはできないので、著作権付きのデータが保護されるのである。そして、このようにして、録音・再生機器に、使用料を予め上乗せしたりせずに、著作権付きデータの保護が図れる利点がある。

【０１４８】さらに、暗号化キーの記録の際は、既存の領域に暗号化キーとなるデータが分散されて記録され、その分散して記録されたデータが寄せ集められて暗号化キーが生成されるので、ディスクのフォーマット方法の変更なしに、暗号化が行なえる利点がある。また、ディスク内での分散方法は、必要に応じて、種々に変更が可能なので、暗号化キーとしての秘匿性は保持され、その強度が高められる利点がある。

【０１４９】そして、また、暗号化キーの生成は、乱数関数Ｒｎｄ（）やハッシュ関数Ｈａｓｈ（）を用いてなされるので、同一のディスクＩＤ等からは同一の暗号化キーが得られるとともに、出力された暗号化キーから元のディスクＩＤ等は解読されなくなる。従って、暗号化キーに関して秘匿性が高まり、著作権付きのデータの二次コピーが防止されるようになる。

（Ａ３）第１実施形態の第３変形例の説明

一方、データを伝送するような別態様の暗号化方法も行なえる。

【０１５０】図１７は、本発明の第１実施形態の第３変形例に係る暗号化・復号化記録装置の模式図である。この図１７に示す暗号化・復号化記録装置４０は、データ送出装置２６と回線３６ａを介して接続されている。この暗号化・復号化記録装置４０は、パソコン２０と、ケーブル４３とをそなえて構成されている。パソコン２０は、暗号化メディア情報生成手段２０ａと、暗号鍵生成手段２０ｂと、復号化手段２０ｃと、第２暗号鍵生成手段２０ｄとをそなえて構成されている。これらのものは、上述したものと同一なものなので、その詳細な説明を省略する。なお、ＣＤ－Ｒ／ＲＷドライブ２２及びケーブル４３は、上述したものと同一のものなので、更なる説明を省略する。また、ＣＤ－Ｒ／ＲＷドライブ２２

40

は、書き込み用ディスク又は再生用ディスクを挿入できる。

【０１５１】また、暗号化キーの生成方法に関しても、第１実施形態にて説明（図３９～図４０参照）したのと同様である。すなわち、暗号化が、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を個別に用いて行なわれたり、又は、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を組み合わせた情報を用いて行なわれるようにしてもよい。

【０１５２】さらに、暗号化が、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を種とする乱数関数を用いてもよく、又は、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を組み合わせた情報を種とする乱数関数を用いて行なうようにもできる。加えて、暗号化が、キーメッセージ，ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を種とするハッシュ関数を用いてもよく、又は、キーメッセージ，ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を組み合わせた情報を種とするハッシュ関数を用いて行なうようにもできる。

【０１５３】また、データ送出装置２６は、データファイル等をこの暗号化・復号化記録装置４０に対して、送出するものであり、例えば、取り込んだアナログデータをＡ／Ｄ変換し、そのディジタルデータを送出するようになっている。さらに、回線３６ａは、データ送出装置２６と暗号化・復号化記録装置４０とを接続する回線であり、例えばパソコン２０のシリアルポート（図示せず）に接続されている。

【０１５４】これにより、例えばアナログデータは、データ送出装置２６において、Ａ／Ｄ変換されて、そのデータが、回線３６ａを介して、暗号化・復号化記録装置４０に入力されて、パソコン２０に、そのシリアルポートから入力される。一方、ＣＤ－Ｒ／ＲＷドライブ２２内の読出手段２２ａにおいて、挿入されたディスクのディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号がメディア番号として読み出され、その読み出されたメディア番号は、ケーブル４３を介して、パソコン２０に入力され、パソコン２０内の暗号鍵生成手段２０ｂにおいて、暗号化キーが生成される。

【０１５５】そして、シリアルポートからのデータは、パソコン２０内の暗号化メディア情報生成手段２０ａにおいて、その暗号化キーを用いて暗号化データが出力され、その暗号化データは、ケーブル４３を介して、ＣＤ－Ｒ／ＲＷドライブ２２に入力される。さらに、その暗号化データは、ＣＤ－Ｒ／ＲＷドライブ２２内の暗号化メディア情報保存手段２２ｂによって、書き込み用ディスクのデータ領域１２ｂ（図１参照）に保存される。

【０１５６】また、書き込み用ディスク又は、再生用ディスクから復号するときは、次のようになる。すなわち、ＣＤ－Ｒ／ＲＷドライブ２２内の第２読出手段２２ｃにおいて、そのディスクＩＤ，ＭＣＮ，ＩＳＲＣのシ

41

リアル番号が読み出され、パソコン２０内の第２暗号鍵生成手段２０ｄにおいて、復号するための暗号化キーが生成され、そして、パソコン２０内の復号化手段２０ｃにおいて、その暗号化データがその暗号化キーを用いて復号されるのである。

【０１５７】このような構成によって、ＣＤ－Ｒ／ＲＷのコピー防止のための、暗号化及び復号化が行なわれる。図１８は、本発明の第１実施形態の第３変形例に係る、ＣＤ－Ｒ又はＣＤ－ＲＷのコピー防止方法のフローチャートである。ステップＥ１から開始される暗号化ステップは、まず、ステップＥ２において、保存するデータが選択された後、そのファイルデータが取り込まれる（ステップＥ３）。なお、このステップまでは、データの状態は、通常のものである。

【０１５８】そして、ステップＥ４において、ＭＣＮ，ＩＳＲＣのシリアル番号，ディスクＩＤを適当に組み合わせた、そのディスク（メディア）固有の暗号化キーによって、そのデータが暗号化され、ステップＥ５において、その暗号化データが書き込み用ディスク（ＣＤ－Ｒ／ＲＷメディア）に保存される。一方、復号ステップとして、ステップＥ６で、そのディスク固有の暗号化キーによって、そのデータが復号され、ステップＥ７で、その復号化データが使用され、ステップＥ８で、暗号化ステップが終了するのである。

【０１５９】また、ステップＥ２において、別のデータを読み出すようにもでき、その場合は、繰り返して、データが選択される。なお、ステップＥ５，Ｅ６において、暗号化データが、暗号化キーとして使用したディスク以外のディスクに書き込まれた場合には、データを復元することはできない。

【０１６０】このように、ユーザが１回目のコピーをするときは、読み込まれた音声，映像，データ等のマルチメディアデータは、ディスク固有の暗号化キーにより、暗号化されて、ユーザは、１枚の特定ディスクを得られる。逆に、ユーザが、その特定ディスクから、他のディスクへコピーをしようとしても、その特定ディスクに格納されている暗号化データを復号するために必要なメディア番号（ディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号）が異なるので、元の音楽や映像データが復元されることはない。

【０１６１】このようにして、音楽や映画等の著作権付きのデータが、１枚のディスクに１回だけコピーできるが、そのコピーされたディスクから他のディスクへ二次コピーすることはできないので、著作権付きのデータが保護されるのである。そして、このようにして、録音・再生機器に、使用料を予め上乗せしたりせずに、著作権付きデータの保護が図れる利点がある。

【０１６２】さらに、暗号化キーの記録の際は、既存の領域に暗号化キーとなるデータが分散されて記録され、その分散して記録されたデータが寄せ集められて暗号化

42

キーが生成されるので、ディスクのフォーマット方法の変更なしに、暗号化が行なえる利点がある。また、ディスク内での分散方法は、必要に応じて、種々に変更が可能なので、暗号化キーとしての秘匿性は保持され、その強度が高められる利点がある。

【０１６３】加えて、暗号化キーの生成は、乱数関数Ｒｎｄ（）やハッシュ関数Ｈａｓｈ（）を用いてなされるので、同一のディスクＩＤ等からは同一の暗号化キーが得られるとともに、出力された暗号化キーから元のディスクＩＤ等は解読されなくなる。従って、暗号化キーに関して秘匿性が高まり、著作権付きのデータの二次コピーが防止されるようになる。

（Ｂ）本発明の第２実施形態の説明

上記の第１実施形態において説明した、暗号化装置及び復号化装置を音響装置に組み込んで使用することもできる。

【０１６４】図１９は、本発明の第２実施形態に係る音響装置の模式図である。この図１９に示す音響装置２７は、暗号化手段と復号化手段とを有する音響装置であって、ＣＤ－Ｒ／ＲＷドライブ４２と、スピーカー２８ａ，２８ｂと、音響再生機器２９とをそなえて構成されている。また、このＣＤ－Ｒ／ＲＷドライブ４２に挿入されるディスクは、初期化された書き込み用ディスクのほかに、データが記録された再生用ディスクである。すなわち、これらのディスク（メディア）は、光学式に記録されるものであり、また、そのデータ領域１２ｂ（図１参照）は、ユーザによって少なくとも１回は書き込まれ得るものである。

【０１６５】ここで、暗号化手段（図示せず）は、音声、データ等の情報を含むマルチメディアデータを暗号化して暗号化メディア情報として記録しうるものであり、復号化手段（図示せず）は、音声、データ等の情報を含むマルチメディアデータが暗号化されて記録された、暗号化メディア情報を復号しうるものである。また、ＣＤ－Ｒ／ＲＷドライブ４２は、音声、データ等の情報を含むマルチメディアデータを暗号化して暗号化メディア情報として記録しうるものであって、読出手段４２ａ，暗号化メディア情報生成手段４２ｂ，暗号化メディア情報保存手段４２ｃ，第２読出手段４２ｄ，第２暗号鍵生成手段４２ｅ，復号化手段４２ｆをそなえて構成されている。

【０１６６】この読出手段４２ａは、初期化された書き込み用ディスク及びデータが記録された再生用ディスクにおけるディスクＩＤを読み出しうるものである。また、この初期化された書き込み用ディスク及びデータが記録された再生用ディスクは、図１に示すディスク１０と同様、ＣＤ－Ｒ／ＲＷドライブ４２が読み出し可能な領域であってユーザはその領域をアクセスできない管理領域１１と、ＣＤ－Ｒ／ＲＷドライブ４２が読み出し可能な領域であってユーザがその領域を任意にアクセスで

きるデータ領域１２ｂとをそなえ、管理領域１１に暗号化のためのディスクＩＤが記録されている。

【０１６７】暗号化メディア情報生成手段４２ｂは、ディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号を用いた暗号化キーによってマルチメディアデータを暗号化し暗号化メディア情報として出力しうるものであり、また、暗号化メディア情報保存手段４２ｃは、その暗号化メディア情報をデータ領域１２ｂ（図１参照）に保存しうるものである。

【０１６８】また、暗号化キーの生成方法に関しても、第１実施形態にて説明（図３９～図４０参照）したのと同様である。すなわち、暗号化が、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を個別に用いて行なわれたり、又は、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を組み合わせた情報を用いて行なわれるようにしてもよい。さらに、暗号化が、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を種とする乱数関数を用いてもよく、又は、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を組み合わせた情報を種とする乱数関数を用いて行なうようにもできる。加えて、暗号化が、キーメッセージ，ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を種とするハッシュ関数を用いてもよく、又は、キーメッセージ，ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を組み合わせた情報を種とするハッシュ関数を用いて行なうようにもできる。

【０１６９】さらに、第２読出手段４２ｄは、書き込み用ディスク及び再生用ディスクにおけるディスクＩＤを読み出しうるものであり、第２暗号鍵生成手段４２ｅは、ディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号から復号のための暗号化キーを生成するものであり、加えて、復号化手段４２ｆは、暗号化された情報をディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号を用いた暗号化キーを用いて復号し、音声、データ等の情報を含むマルチメディアデータを再生しうるものである。

【０１７０】これらの機能のうち、読出手段４２ａ，暗号化メディア情報保存手段４２ｃ，第２読出手段４２ｄは、ＣＤ－Ｒ／ＲＷドライブ４２内のドライブ装置によって発揮される。一方、暗号化メディア情報生成手段４２ｂ，第２暗号鍵生成手段４２ｅ，復号化手段４２ｆの機能は、例えば、内部に組み込まれたソフトウェア等により発揮される。

【０１７１】また、スピーカー２８ａは、ステレオ音声の左チャネル用のスピーカーであり、スピーカー２８ｂは、ステレオ音声の右チャネル用のスピーカーである。さらに、音響再生機器２９は、音楽データを読み出して、再生し、増幅して、スピーカー２８ａ，２８ｂから出力しうるものである。これにより、暗号化は次のようになる。すなわち、書き込み用ディスクは、ＣＤ－Ｒ／ＲＷドライブ４２内の読出手段４２ａにおいて、挿入されたディスクのディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号がメディア番号として読み出される。そして、ＣＤ－Ｒ／ＲＷドライブ４２内の暗号化メディア情報生成手段４２ｂにおいて、ディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号を用いた暗号化キーによってマルチメディアデータが暗号化され、暗号化メディア情報として出力される。そして、ＣＤ－Ｒ／ＲＷドライブ４２内の暗号化メディア情報保存手段４２ｃにおいて、その暗号化メディア情報は、書き込み用ディスクのデータ領域１２ｂ（図１参照）に保存される。

【０１７２】さらに、復号化については、次のようになる。すなわち、ＣＤ－Ｒ／ＲＷドライブ４２内の第２読出手段４２ｄにおいて、書き込み用ディスク又は、再生用ディスクから、ディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号が読み出され、また、第２暗号鍵生成手段４２ｅにおいて、ディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号から暗号化キーが生成され、さらに、復号化手段４２ｆにおいて、その暗号化キーによって、その暗号化メディア情報が復号されるのである。

【０１７３】このような構成によって、ユーザは、この音響装置２７に格納された音楽データを再生するとともに、ＣＤ－Ｒ／ＲＷの違法コピー防止のための暗号化及び復号化を行なう。すなわち、音楽データは、適当に再生・増幅がされて、左右のスピーカー２８ａ，２８ｂから出力される。

【０１７４】一方、ユーザがコピーする場合は、まず、音楽データが、読み込まれ、その読み込まれた音楽データは、記録すべき書き込み用ディスクにコピーされる際に、その書き込み用ディスク固有のＭＣＮ，ＩＳＲＣのシリアル番号，ディスクＩＤによって、ディスク固有の暗号化キーが作成されて、これらの暗号化キーにより、音楽データは暗号化される。その暗号化データは、元の暗号化キーが読み出されたディスク以外の、複数のディスクにコピーされたとしても、ディスク固有の暗号化キーが異なるので、元の音楽データが復元されることはない。従って、特定ディスクのみ、元のデータを再生することができる。

【０１７５】このように、ユーザが１回目のコピーをするときは、読み込まれた音楽データや音声データは、ディスク固有の暗号化キーにより、暗号化されて、ユーザは、１枚の特定ディスクを得られる。逆に、ユーザが、その特定ディスクから、他のディスクへコピーをしようとしても、その特定ディスクに格納されている暗号化データを復号するために必要なメディア番号（ディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号）が異なるので、元の音楽データ等が復元されることはない。

【０１７６】このようにして、音楽等の著作権付きのデータが、１枚のディスクに１回だけコピーできるが、そのコピーされたディスクから他のディスクへ二次コピーすることはできないので、著作権付きのデータが保護さ

45

れるのである。そして、このようにして、録音・再生機器に、使用料を予め上乗せしたりせずに、著作権付きデータの保護が図れる利点がある。

【０１７７】また、暗号化キーを記録する際には、ＣＤ－Ｒディスクあるいは ＣＤ－ＲＷディスク内の管理領域１１とデータ領域１２ｂ（図１参照）とが利用され、これらの領域に暗号化キーとなるデータが分散されて記録され、その分散して記録されたデータが寄せ集められて暗号化キーが生成されるので、既存のディスクのフォーマット方法を変更せずに、暗号化が行なえるようになる。加えて、その分散方法は、必要に応じて、種々に変更させることができるので、暗号化キーとしての強度を高めることができるのである。

【０１７８】なお、再生だけ行なうような態様でも可能である。図２０は、本発明の第２実施形態に係る他の音響装置の模式図である。この図２０に示す音響装置２７ａは、音声、データ等の情報を含むマルチメディアデータが暗号化されて記録された、暗号化メディア情報を復号しうる復号化手段（図示せず）を有するものであって、ＣＤ－Ｒ／ＲＷドライブ４３と、スピーカー２８ａ，２８ｂとをそなえて構成されている。

【０１７９】また、暗号化キーの生成方法に関しても、第１実施形態にて説明（図３９～図４０参照）したのと同様である。すなわち、暗号化が、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を個別に用いて行なわれたり、又は、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を組み合わせた情報を用いて行なわれるようにしてもよい。さらに、暗号化が、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を種とする乱数関数を用いてもよく、又は、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を組み合わせた情報を種とする乱数関数を用いて行なうようにもできる。加えて、暗号化が、キーメッセージ，ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を種とするハッシュ関数を用いてもよく、又は、キーメッセージ，ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を組み合わせた情報を種とするハッシュ関数を用いて行なうようにもできる。

【０１８０】また、挿入されるディスクは、暗号化キーによって生成された、暗号化データが記録されているディスクである。ここで、ＣＤ－Ｒ／ＲＷドライブ４３は、ＣＤ－Ｒディスク２１ａ，３１ａ又はＣＤ－ＲＷディスク２１ｂ，３１ｂの暗号化キーを用いて、これらのディスク（メディア）に暗号化されて記録されている音声，データ等のマルチメディアデータを、復号するものであり、第２読出手段４２ｄ，第２暗号鍵生成手段４２ｅ，復号化手段４２ｆをそなえて構成されている。なお、スピーカー２８ａ，２８ｂは、上述したものと同一のものである。

【０１８１】このような構成によって、音楽の再生が行

46

なわれる一方、復号が行なわれる。すなわち、ＣＤ－Ｒ／ＲＷドライブ４３内の第２読出手段４２ｄにおいて、再生用ディスクのディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号が読み出され、第２暗号鍵生成手段４２ｅにおいて、暗号化キーが生成され、復号化手段４２ｆにおいて、再生用ディスクの暗号化データがその暗号化キーを用いて復号され、そして、音声，データ等のマルチメディアデータが再生されるのである。

【０１８２】ここで、このディスク以外のディスクに暗号化されて記録されたデータは、ディスク固有の暗号化キーが異なるので、元の音楽データが復元されることはなく、一枚のディスクにのみ記録された情報のみが再生されるのである。このように、ユーザは、ディスク固有の暗号化キーにより、復号して再生をするので、その暗号化キー以外の暗号化キーでは、元の音楽データ等を復元することはできない。

【０１８３】このようにして、音楽等の著作権付きのデータが、１枚のディスクに１回だけコピーできるが、そのコピーされたディスクから他のディスクへ二次コピーすることはできないので、著作権付きのデータが保護されるのである。そして、このようにして、録音・再生機器に、使用料を予め上乗せしたりせずに、著作権付きデータの保護が図れる利点がある。

【０１８４】さらに、暗号化キーの記録の際は、既存の領域に暗号化キーとなるデータが分散されて記録され、その分散して記録されたデータが寄せ集められて暗号化キーが生成されるので、ディスクのフォーマット方法の変更なしに、暗号化が行なえる利点がある。また、ディスク内での分散方法は、必要に応じて、種々に変更が可能なので、暗号化キーとしての秘匿性は保持され、その強度が高められる利点がある。

【０１８５】加えて、暗号化キーの生成は、乱数関数Ｒｎｄ（）やハッシュ関数Ｈａｓｈ（）を用いてなされるので、同一のディスクＩＤ等からは同一の暗号化キーが得られるとともに、出力された暗号化キーから元のディスクＩＤ等は解読されなくなる。従って、暗号化キーに関して秘匿性が高まり、著作権付きのデータの二次コピーが防止されるようになる。

（Ｂ１）本発明の第２実施形態の第１変形例の説明

第２実施形態において説明した、暗号化及び復号しうる機能を、映像機器に組み込んで使用することもできる。

【０１８６】図２１は、本発明の第２実施形態の第１変形例に係る音響・映像・データ装置の模式図である。この図２１に示す音響・映像・データ装置３２は、音声、映像、データ等の情報を含むマルチメディアデータを暗号化して暗号化メディア情報として記録しうるとともに、音声、映像、データ等の情報を含むマルチメディアデータが暗号化されて記録された、暗号化メディア情報を復号しうるものであって、ＣＤ－Ｒ／ＲＷドライブ付きテレビ３３と、ＡＶ装置３４と、スピーカー２８ａ，

２８ｂとをそなえて構成されている。また、挿入されるディスクは、初期化された書き込み用ディスクか、あるいは、既にデータを書き込んだ状態の再生用ディスクを挿入して音声や映像データを再生することも可能である。

【０１８７】ここで、ＣＤ－Ｒ／ＲＷドライブ付きテレビ３３は、テレビの機能を有するほかに、ＣＤ－Ｒディスク２１ａ又はＣＤ－ＲＷディスク２１ｂの暗号化キーを用いて、音声データ又は音楽データを、暗号化して、その暗号化したデータを記録する機能を有するものであって、読出手段４２ａ，暗号化メディア情報生成手段４２ｂ，暗号化メディア情報保存手段４２ｃ，第２読出手段４２ｄ，第２暗号鍵生成手段４２ｅ，復号化手段４２ｆをそなえて構成されている。これらは、第２実施形態にて説明した機能に加えて、映像データを処理する機能を有するものであって、更なる説明を省略する。

【０１８８】また、暗号化の生成方法に関しても、第１実施形態にて説明（図３９～図４０参照）したのと同様である。すなわち、暗号化が、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を個別に用いて行なわれたり、又は、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を組み合わせた情報を用いて行なわれるようにしてもよい。さらに、暗号化が、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を種とする乱数関数を用いてもよく、又は、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を組み合わせた情報を種とする乱数関数を用いて行なうようにもできる。加えて、暗号化が、キーメッセージ，ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を種とするハッシュ関数を用いてもよく、又は、キーメッセージ，ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を組み合わせた情報を種とするハッシュ関数を用いて行なうようにもできる。

【０１８９】また、ＡＶ(Audio-Visual)装置３４は、音声や映像のデータを再生できるものであって、例えば、ビデオ再生装置である。なお、スピーカー２８ａ，２８ｂは、上述したものと同様である。また、ケーブル４３ｂ，４３ｃ，４３ｄは、これらの機器の間を電気的に接続するものである。これにより、ＣＤ－Ｒ／ＲＷドライブ付きテレビ３３内の読出手段４２ａにおいて、書き込み用ディスクのディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号がメディア番号として読み出される。

【０１９０】一方、ＡＶ装置３４において、音声や映像のデータが再生され、この再生された音声や映像のデータは、ケーブル４３ｄを介して、このＣＤ－Ｒ／ＲＷドライブ付きテレビ３３に入力され、そのデータは、適当に再生・増幅がされて、ケーブル４３ｂ，４３ｃを介して、左右のスピーカー２８ａ，２８ｂから出力される。

【０１９１】また、一方、このＣＤ－Ｒ／ＲＷドライブ付きテレビ３３内の暗号化メディア情報生成手段４２ｂ

において、ディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号によって、ディスク固有の暗号化キーが作成されて、その音楽等のデータは、その暗号化キーを用いて暗号化データが出力される。そして、その暗号化データは、ＣＤ－Ｒ／ＲＷドライブ付きテレビ３３内の暗号化メディア情報保存手段４２ｃによって、書き込み用ディスクのデータ領域１２ｂに保存される。

【０１９２】さらに、復号化については、次のようになる。すなわち、ＣＤ－Ｒ／ＲＷドライブ付きテレビ３３内の第２読出手段４２ｄにおいて、ディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号が読み出され、また、第２暗号鍵生成手段４２ｅにおいて、ディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号から暗号化キーが生成され、さらに、復号化手段４２ｆにおいて、その暗号化キーによって、その暗号化データが復号され、そして、音声，映像，データ等のマルチメディアデータが再現されるのである。

【０１９３】このような構成によって、ユーザは、この音響・映像・データ装置３２に格納された音楽や映像の情報を再生するとともに、ＣＤ－Ｒ／ＲＷの違法コピー防止のための暗号化された音声データや映像データのコピーを行なう。すなわち、ユーザが１回目のコピーをするときは、まず、音声や映像の情報が、読み込まれ、その読み込まれた音声や映像の情報は、ディスク固有の暗号化キーにより、暗号化される。従って、ユーザは、１枚の特定ディスクを得られる。

【０１９４】逆に、ユーザが、その特定ディスクから、他のディスクへコピーをしようとしても、その特定ディスクに格納されている暗号化データを復号するために必要なメディア番号（ディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号）が異なるので、元の音楽や映像データが復元されることはない。このようにして、一枚のディスクにのみ、記録されるので、著作物データは、違法にコピーされることがなくなる。

【０１９５】加えて、乱数関数Ｒｎｄ（）やハッシュ関数Ｈａｓｈ（）を用いて暗号化が行なわれることにより、同一のディスクＩＤ等からは同一の暗号化キーが得られるようになり、また、元のディスクＩＤ等の解読はできなくなって、秘匿性が高まる。

（Ｂ２）本発明の第２実施形態の第２変形例の説明

一方、再生だけの場合は、次のようになる。

【０１９６】図２２は、本発明の第２実施形態の第２変形例に係る音響・映像・データ装置の模式図である。この図２２に示す音響・映像・データ装置３２ａは、音声、映像、データ等の情報を含むマルチメディアデータが暗号化されて記録された、暗号化メディア情報を復号，再生しうるものであって、ＣＤ－Ｒ／ＲＷドライブ付きテレビ３３とスピーカー２８ａ，２８ｂとをそなえて構成されている。

【０１９７】このＣＤ－Ｒ／ＲＷドライブ付きテレビ３

３は、ＣＤ－ＲディスクまたはＣＤ－ＲＷディスクの暗号化キーを用いて、これらのディスクに暗号化されて記録されている音声，映像，データ等のマルチメディアデータを、復号するものであり、第２読出手段４２ｄ，第２暗号鍵生成手段４２ｅ，復号化手段４２ｆをそなえて構成されている。これらは、上述したものと同一であるので、更なる説明を省略する。

【０１９８】また、暗号化の生成方法に関しても、第１実施形態にて説明（図３９～図４０参照）したのと同様である。すなわち、暗号化が、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を個別に用いて行なわれたり、又は、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を組み合わせた情報を用いて行なわれるようにしてもよい。さらに、暗号化が、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を種とする乱数関数を用いてもよく、又は、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を組み合わせた情報を種とする乱数関数を用いて行なうようにもできる。加えて、暗号化が、キーメッセージ，ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を種とするハッシュ関数を用いてもよく、又は、キーメッセージ，ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を組み合わせた情報を種とするハッシュ関数を用いて行なうようにもできる。

【０１９９】また、挿入されるディスクは、暗号化キーによって生成された、暗号化データが記録されている再生用ディスクである。これにより、ＣＤ－Ｒ／ＲＷドライブ付きテレビ３３内の第２読出手段４２ｄにおいて、再生用ディスクのディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号が読み出され、第２暗号鍵生成手段４２ｅにおいて、暗号化キーが生成される。そして、復号化手段４２ｆにおいて、再生用ディスクの暗号化データが、その暗号化キーを用いて復号されるのである。

【０２００】このような構成によって、ＣＤ－Ｒ／ＲＷドライブ付きテレビ３３は、再生用ディスクのコピー防止がなされる。すなわち、このディスク以外のディスクに暗号化されて記録されたデータは、ディスク固有の暗号化キーが異なるので、元の音楽や映像データが復元されることはなく、一枚のディスクにのみ記録された情報のみが再生されるのである。

【０２０１】このようにして、音楽や映画等の著作権付きのデータは、１枚のディスクから他のディスクへ二次コピーされることはできないので、著作権付きのデータが保護されるのである。そして、このようにして、録音・再生機器に、使用料を予め上乗せしたりせずに、著作権付きデータの保護が図れる利点がある。さらに、暗号化キーの記録の際は、既存の領域に暗号化キーとなるデータが分散されて記録され、その分散して記録されたデータが寄せ集められて暗号化キーが生成されるので、ディスクのフォーマット方法の変更なしに、暗号化が行なえる利点がある。また、ディスク内での分散方法は、必要に応じて、種々に変更が可能なので、暗号化キーとしての秘匿性は保持され、その強度が高められる利点がある。

【０２０２】加えて、乱数関数Ｒｎｄ（）やハッシュ関数Ｈａｓｈ（）を用いて暗号化が行なわれるので、同一のディスクＩＤ等からは同一の暗号化キーが得られる。また、元のディスクＩＤ等の解読ができなくなるので、秘匿性が高まる。

（Ｃ）本発明の第３実施形態の説明

その他の応用例について、さらに説明する。

【０２０３】図２３は、本発明の第３実施形態に係る暗号化・復号化記録装置を示す図である。この図２３に示す暗号化・復号化記録装置４０ｂは、ＣＤ－ＲディスクまたはＣＤ－ＲＷディスクの暗号化キーを用いて、ディジタルデータの暗号化を行なって、ＣＤ－ＲディスクまたはＣＤ－ＲＷディスクへの記録をし、また、ＣＤ－ＲディスクまたはＣＤ－ＲＷディスクに記録された暗号化データを復号してその復号化データを取り出すものである。そして、この暗号化・復号化記録装置４０ｂは、周辺記憶装置３５と、パソコン２０と、ＣＤ－Ｒ／ＲＷドライブ２２とをそなえて構成されている。また、付加機能として、この暗号化・復号化記録装置４０ｂは、暗号化方法を任意に変更できるものである。

【０２０４】この周辺記憶装置３５は、データを蓄積するものであって、例えば、ハードディスクやＭＯドライブのようなものであり、この中に格納しているデータが暗号化方法の選択に使用されるようになっている。この暗号化方法の選択とは、ＤＥＳ，ＲＣ４，ＩＤＥＡ等の中から任意に選択することを意味する。また、パソコン２０，ＣＤ－Ｒ／ＲＷドライブ２２は、上述した第１実施形態の第１変形例で説明したものと同一である。さらに、挿入されるディスクは、初期化されたディスクである。また、これらの機器の間は、ケーブル４３ａ，４３ｂによって、接続されている。

【０２０５】なお、ＣＤ－Ｒ／ＲＷドライブ２２、ケーブル４３ａ，４３ｂは、上述したものと同一であるので、更なる説明を省略する。これにより、ＣＤ－Ｒ／ＲＷドライブ２２内の読出手段２２ａにおいて、挿入されたディスクのディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号がメディア番号として読み出され、その読み出されたメディア番号は、ケーブル４３ｂを介して、パソコン２０に入力され、パソコン２０内の暗号鍵生成手段２０ｂにおいて、周辺記憶装置３５から取り込まれたデータに基づく暗号化方法で、暗号化キーが生成される。

【０２０６】また、暗号化キーの生成方法に関しても、第１実施形態にて説明（図３９～図４０参照）したのと同様である。すなわち、暗号化が、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を個別に用いて行なわれたり、又は、ディスクＩＤ，ＭＣＮ若しくはＩＳＲ

Ｃのシリアル番号を組み合わせた情報を用いて行なわれるようにしてもよい。さらに、暗号化が、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を種とする乱数関数を用いてもよく、又は、ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を組み合わせた情報を種とする乱数関数を用いて行なうようにもできる。加えて、暗号化が、キーメッセージ，ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を種とするハッシュ関数を用いてもよく、又は、キーメッセージ，ディスクＩＤ，ＭＣＮ若しくはＩＳＲＣのシリアル番号を組み合わせた情報を種とするハッシュ関数を用いて行なうようにもできる。

【０２０７】そして、パソコン２０内の暗号化メディア情報生成手段２０ａにおいて、その暗号化キーで暗号化された暗号化データが出力され、この暗号化データは、ＣＤ－Ｒ／ＲＷドライブ２２内の暗号化メディア情報保存手段２２ｂによって、書き込み用ディスクのデータ領域１２ｂ（図１参照）に保存される。ここで、この暗号化・復号化記録装置４０ｂを操作するユーザは、暗号化方法を変更するときには、周辺記憶装置３５から、別の暗号にするためのデータを、ケーブル４３ａを介して、パソコン２０内に取り込む。そして、別の暗号化方法にすることで、暗号化キーを変えられるようになるのである。

【０２０８】さらに、書き込み用ディスク又は、再生用ディスクから復号するときは、次のようになる。すなわち、ＣＤ－Ｒ／ＲＷドライブ２２内の第２読出手段２２ｃにおいて、そのディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号が読み出され、パソコン２０内の復号化手段２０ｃにおいて、書き込み用ディスク又は、再生用ディスクの暗号化データが暗号化キーを用いて復号されるのである。

【０２０９】このような構成によって、ユーザは、この暗号化・復号化記録装置４０ｂに格納された暗号化方法を変えるためのプログラム等を使用できるとともに、それを用いてＣＤ－Ｒ／ＲＷの違法コピー防止のための暗号化されたディジタルデータのコピーを行なう。すなわち、ユーザは、暗号化方法を、例えばＤＥＳからＲＣ４に変更するために、周辺記憶装置３５から、その暗号化のためのプログラム等を取り込んで、暗号化方法を変える。また、この変更は、自由に行なうことができる。

【０２１０】そして、上述したものと同様に、ユーザは、１回目のコピーをするときは、まず、ディジタルデータを読み込み、その読み込まれたディジタルデータを、ディスク固有の暗号化キーにより、暗号化する。従って、ユーザは、１枚の特定ディスクを得られる。逆に、ユーザが、その特定ディスクから、他のディスクへコピーをしようとしても、その特定ディスクに格納されている暗号化データを復号するために必要なメディア番号（ディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号）が異なるので、元のディジタルデータが復元されることはない。

【０２１１】このように、暗号化方法が、必要に応じて、種々に変更可能なので、暗号としての秘匿性が保持され、その強度を高めることができる利点がある。また、このようにして、音楽や映画等の著作権付きを含めたディジタルデータが、１枚のディスクに１回だけコピーできるが、そのコピーされたディスクから他のディスクへ二次コピーすることはできないので、著作権付きのデータが保護される。そして、このようにして、録音・再生機器に、使用料を予め上乗せしたりせずに、著作権付きデータの保護が図れる利点がある。

【０２１２】さらに、暗号化キーの記録の際は、既存の領域に暗号化キーとなるデータが分散されて記録され、その分散して記録されたデータが寄せ集められて暗号化キーが生成されるので、ディスクのフォーマット方法の変更なしに、暗号化が行なえる利点がある。また、ディスク内での分散方法は、必要に応じて、種々に変更が可能なので、暗号化キーとしての秘匿性は保持され、その強度が高められる利点がある。

【０２１３】加えて、乱数関数Ｒｎｄ（）やハッシュ関数Ｈａｓｈ（）を用いて暗号化が行なわれるので、同一のディスクＩＤ等からは同一の暗号化キーが得られる。また、元のディスクＩＤ等の解読ができなくなるので、秘匿性が高まる。

（Ｄ）その他

本発明は上述した実施態様及びその変形例に限定されるものではなく、本発明の趣旨を逸脱しない範囲で、種々変形して実施することができる。

【０２１４】まず、上述した、暗号化キーの長さの違いによる、暗号化キーの、組み合わせの仕方は、その他の態様でも行なえる。ディスクＩＤは、ハードウェアによっては、読み取りができないことがあるので、その場合には、ＭＣＮとＩＳＲＣのシリアル番号との２種類を併せて使用することもでき、簡易な暗号化ができるようになる。

【０２１５】加えて、ＭＤ方式の短所は、安全性の理論的根拠が確立されておらず、その上、並列処理を導入することが困難である点である。そして、１２８ビットのハッシュアルゴリズム（ＭＤ５）を使用するときは、同一のメッセージダイジェストを生成する確率を低下させるために、好ましくは、元のディスクＩＤ等を組み合わせたものは、１２８ビット以上のビット長とする。

【０２１６】また、本発明で使用したユーザという語は、二次メーカーや、一般消費者等を意味するだけでなく、初期化されたディスクをデータ等の記録のために使用するような者も含むものである。さらに、第１実施形態の第１変形例で説明した、回線３６は、ローカルエリアネットワークに限らずに、電話回線を用いたいわゆるダイアルアップ接続のような回線をも含むものである。

そして、暗号化のための暗号化キーが生成される箇所は、インターネットサーバ２３でなくとも、パソコン２０でも可能であり、その場合、暗号化キーだけをインターネットサーバ２３に送信するようにする。加えて、この場合は、通信カラオケにおける、データ送出機と、受信端末との間での情報をやり取りするように、応用することも可能である。

【０２１７】そして、第１実施形態の第２変形例で説明した、データ送出装置２６と、パソコン２０とを接続する回線３６ａは、シリアルポートに限らずに、他のポートを使用することも可能であり、さらに、無線を用いて、データを伝送するようにもできる。加えて、第２実施形態に第１変形例において、ＡＶ装置３４としては、ビデオ再生装置に限らずに、衛星放送や地上波の電波受信装置であったり、また、ＣＡＴＶ等の家庭内端末であってもよい。

【０２１８】なお、図８，９，１０において、チャンネルと表示されているものは、チャネルを意味し、これらは同一の意味である。さらに、図１４で、ＰＣと表示されているものは、パソコン２０を意味する。また、図１４，１６，１８において、暗号キーと表示されているものは、暗号化キーを意味している。加えて、図２４，２５，２６に表示されているΦは、ミリメートル単位の直径の長さを表す記号である。

【０２１９】また、以上の説明では、ＣＤ－Ｒ／ＲＷを例としたが、本発明は、ＣＤ－Ｒ／ＲＷに限定することなく他の媒体にも適用可能である。例えば、ＤＶＤ－Ｒ，ＤＶＤ－ＲＡＭ，ＤＶＤ－ＲＷなどの媒体においても管理領域にディスク情報を記録することができる。なお、２層型媒体や両面型媒体であれば、管理領域は、うち一層或いは一面のみに設けてもよく、各層或いは各面に設けてもよい。

【０２２０】

【発明の効果】以上詳述したように、本発明の記録媒体によれば、読み取り装置が読み出し可能な領域であってユーザはその領域をアクセスできない管理領域と、読み取り装置が読み出し可能な領域であってユーザがその領域を任意にアクセスできるデータ領域とをそなえ、その管理領域に、暗号化のためのディスク識別情報が記録されているので、ユーザは、１枚だけは特定ディスクを得られるが、ユーザが、その特定ディスクから、他のディスクへコピーをしようとしても、その特定ディスクに格納されている暗号化データを復号するために必要なメディア番号（ディスクＩＤ，ＭＣＮ，ＩＳＲＣのシリアル番号）が異なるので、元の音楽や映像データが復元されず、そのコピーされたディスクから他のディスクへ二次コピーすることはできないので、著作権付きのデータが保護される利点がある。さらに、録音・再生機器に、使用料を予め上乗せしたりせずに、著作権付きデータの保護が図れる利点がある。加えて、ディスクの既存のフォーマット方法を変更しないで暗号化が行なえる利点があり、また、暗号化キーの分散方法は、必要に応じて、種々に変更可能なので、暗号化キーとしての秘匿性が保持され、その強度を高めることができる利点がある（請求項１）。

【０２２１】加えて、本発明によれば、以下に示す①～④のような効果ないし利点がある。

①本発明は、暗号化のためのディスク識別情報が、ディスクに記録される点で、コピー防止のための特定の値が、媒体の特定部分記録される公知文献１記載の技術と異なり、従って、本発明は、単なるコピー防止ではなく、データを暗号化できるようになり、これにより、データ保護の信頼性が非常に高くなるという利点がある。

【０２２２】②本発明は、暗号化のためのディスク識別情報が、「読み取り装置が読み出し可能な領域であってユーザはその領域をアクセスできない管理領域」に記録される点で、暗号化のキー情報が、バーコードや幾何学模様により非データ記録領域に記録される公知文献２記載の技術と異なり、従って、本発明によれば、専用のキー情報読み取り手段を使用しないで暗号化が行なえる利点がある。

【０２２３】③本発明は、記録可能なディスクにおいて、ディスク毎に異なるディスク識別情報が、「読み取り装置が読み出し可能な領域であってユーザはその領域をアクセスできない管理領域」に記録される点で、暗号化データ及び暗号化キー情報が、それぞれ、記録形式又は記録層が異なる２つの記録領域に記録される公知文献３記載の技術と異なり、従って、本発明によれば、ディスク個別に暗号化キーの設定が行なえて、データ保護の信頼性が非常に高くなる利点があり、専用のキー情報読み取り手段を使用しないで暗号化が行なえる利点がある。

【０２２４】④本発明は、暗号化のためのディスク識別情報を記録すべき領域が、具体的に「読み取り装置が読み出し可能な領域であってユーザはその領域をアクセスできない管理領域」とされている点で、ＴＯＣ領域が、ユーザが書き換えようとすれば任意にその領域の情報を書き換え／消去を可能とする公知文献４記載の技術とは異なり、従って、本発明によれば、ユーザによるデータの暗号化キーの改竄の可能性が非常に低くできる利点がある。

【０２２５】また、そのデータ領域に、音声、映像、データ等のメディア情報が、少なくとも上記のディスク識別情報を用いて生成された暗号鍵によって暗号化された暗号化メディア情報として記録されるとともに、ユーザが読み出しうる媒体識別番号情報が、分散されて記録されるように構成することもでき、そのようにすれば、他のディスクへコピーをしようとしても、その特定ディスクに格納されている暗号化データを復号するために必要なメディア番号（ディスクＩＤ，ＭＣＮ，ＩＳＲＣのシ

リアル番号）が異なるので、元の音楽や映像データが復元されず、そのコピーされたディスクから他のディスクへ二次コピーすることはできないので、著作権付きのデータが保護される利点がある（請求項２）。

【０２２６】さらに、本発明の記録媒体の初期化方法によれば、読み取り装置が読み出し可能な領域であってユーザはその領域をアクセスできない管理領域と、読み取り装置が読み出し可能な領域であってユーザがその領域を任意にアクセスできるデータ領域とをそなえた記録媒体の初期化方法であって、管理領域に暗号化のためのディスク識別情報を記録するように構成されており、また、管理領域に暗号化のためのディスク識別情報を記録する第１書込ステップと、データ領域にＱチャネルサブコードのモード２形式で媒体識別番号情報を記録する第２書込ステップと、データ領域にＱチャネルサブコードのモード３形式でシリアル番号情報を記録する第３書込ステップとをそなえて構成されてもよく、このようにすれば、やはり、そのコピーされたディスクから他のディスクへ二次コピーすることはできず、著作権付きのデータが保護される利点がある。加えて、ディスクの既存のフォーマット方法を変更しないで暗号化が行なえる利点があり、また、暗号化キーの分散方法は、必要に応じて、種々に変更可能なので、暗号化キーとしての秘匿性が保持され、その強度を高めることができる利点がある（請求項５，６）。

【０２２７】そして、本発明の記録媒体上での暗号化方法によれば、管理領域に暗号化のためのディスク識別情報を記録する初期化を行なった後に、音声、映像、データのいずれか一つの情報を含むメディア情報を、少なくとも上記のディスク識別情報を用いた暗号鍵によって暗号化し、暗号化メディア情報としてデータ領域に記録することにより、特定記録媒体を生成する暗号化ステップをそなえて構成されているので、音楽や映画等の著作権付きのデータが、１枚のディスクに１回だけコピーできるが、そのコピーされたディスクから他のディスクへ二次コピーすることはできないので、著作権付きのデータが保護される利点がある。そして、録音・再生機器に、使用料を予め上乗せしたりせずに、著作権付きデータの保護が図れる利点がある（請求項７）。

【０２２８】また、その初期化は、管理領域に暗号化のためのディスク識別情報を記録する第１書込ステップと、データ領域にＱチャネルサブコードのモード２形式で媒体識別番号情報を記録する第２書込ステップと、データ領域にＱチャネルサブコードのモード３形式でシリアル番号情報を記録する第３書込ステップとから構成され、その暗号化ステップが、ディスク識別情報を第１ディスク識別情報として読み出す第１ディスク識別情報読出ステップと、第１ディスク識別情報と、媒体識別番号情報及びシリアル番号情報のうちの少なくとも一つの情報とを組み合わせて第１暗号鍵を生成する第１暗号鍵生成ステップと、外部装置よりメディア情報を読み出す第１読出ステップと、第１暗号鍵を用いて暗号化メディア情報を生成し、第１ディスク識別情報を有するデータ領域に記録することにより、特定記録媒体を生成する特定記録媒体生成ステップとをそなえて構成されてもよく、このようにすれば、そのコピーされたディスクから他のディスクへ二次コピーすることはできず、著作権付きのデータが保護される利点がある（請求項８，９）。

【０２２９】加えて、本発明の暗号化装置によれば、初期化された記録媒体が、読出手段において、少なくともディスク識別情報が読み出され、暗号化メディア情報生成手段において、データ領域に少なくとも上記のディスク識別情報を用いた暗号鍵によって音声、映像、データ等のメディア情報が暗号化され、暗号化メディア情報保存手段において、暗号化メディア情報が、同一のディスク識別情報を有する記録媒体のデータ領域に保存されるように構成されているので、やはり、そのコピーされたディスクから他のディスクへ二次コピーすることはできず、著作権付きのデータが保護される利点がある（請求項１０）。

【０２３０】また、本発明の復号化装置によれば、暗号化された情報が記録された記録媒体が、第２読出手段において、少なくともディスク識別情報が読み出され、第２暗号鍵生成手段において、少なくともディスク識別情報から第２暗号鍵が生成され、復号化手段において、暗号化された情報が第２暗号鍵を用いて復号され、音声、映像、データ等のメディア情報が再生されるように構成されているので、ディスクの既存のフォーマット方法を変更しないで暗号化が行なえる利点があり、また、暗号化キーの分散方法は、必要に応じて、種々に変更可能なので、暗号化キーとしての秘匿性が保持され、その強度を高めることができる利点がある（請求項１１）。

【０２３１】さらに、本発明の音響・映像・データ装置によれば、初期化された記録媒体に、音声、映像、データ等のメディア情報を暗号化して暗号化メディア情報として記録しうるとともに、暗号化された情報が記録された記録媒体が、少なくともディスク識別情報から生成される第２暗号鍵を用いて復号され音声、映像、データ等のメディア情報が再生されるので、そのコピーされたディスクから他のディスクへ二次コピーすることはできないので、著作権付きのデータが保護される利点がある。また、ディスクの既存のフォーマット方法を変更しないで暗号化が行なえる利点があり、また、暗号化キーの分散方法は、必要に応じて、種々に変更可能なので、暗号化キーとしての秘匿性が保持され、その強度を高めることができる利点がある（請求項１２，１３）。

【０２３２】また、上記の記録媒体は、光学式に記録されてもよく、データ領域が、ユーザによって少なくとも１回は書き込まれ得るものでもよく、従って、このようにすれば、そのコピーされたディスクから他のディスク

57

へ二次コピーすることはできないので、著作権付きのデータが保護される利点がある（請求項３，４）。加えて、上記の暗号化は、ディスク識別情報，媒体識別番号情報並びにシリアル番号情報又はこれらを組み合わせた情報を用いて行なわれるようにしてもよく、また、ディスク識別情報，媒体識別番号情報並びにシリアル番号情報又はこれらを組み合わせた情報を種とする乱数関数を用いて行なわれるようにしてもよく、さらに、キーメッセージ，ディスク識別情報，媒体識別番号情報並びにシリアル番号情報又はこれらを組み合わせた情報を種とするハッシュ関数を用いて行なわれるようにしてもよく、このようにすれば、元のディスク識別情報等が復元されないので、メディア情報の秘匿性が高まり、著作権付きデータが保護されるようになる（請求項１４～請求項２０）。

【図面の簡単な説明】

【図１】本発明が適用される、ＣＤ－Ｒ／ＲＷの非データ領域と、データ領域との配置を示す図である。

【図２】（ａ）は初期化されたＣＤ－Ｒ／ＲＷの概念的な領域配置を示す図であり、（ｂ）は暗号化データが記録されたＣＤ－Ｒ／ＲＷの概念的な領域配置を示す図である。

【図３】メディア番号により暗号化されることを説明するための図である。

【図４】メディア番号により復号化されることを説明するための図である。

【図５】二次コピーができないことを説明するための図である。

【図６】暗号化キーを用いた暗号化方法を示す図である。

【図７】本発明の第１実施形態に係る暗号化キー刷り込み装置の模式図である。

【図８】本発明の第１実施形態に係る、ＣＤ－ＲＷのコピー防止方法における初期化フローチャートである。

【図９】本発明の第１実施形態に係る、ＣＤ－Ｒのコピー防止方法における初期化フローチャートである。

【図１０】本発明の第１実施形態に係る、ＣＤ－Ｒのコピー防止方法における初期化フローチャートである。

【図１１】本発明の第１実施形態に係る、ＣＤ－Ｒのコピー防止方法における初期化フローチャートである。

【図１２】本発明の第１実施形態に係る初期化後のＣＤ－Ｒ／ＲＷのデータレイアウトを示す図である。

【図１３】本発明の第１実施形態の第１変形例に係る暗号化・復号化キー記録装置の模式図である。

【図１４】本発明の第１実施形態の第１変形例に係る、ＣＤ－Ｒ又はＣＤ－ＲＷのコピー防止方法のフローチャートである。

【図１５】本発明の第１実施形態の第２変形例に係る暗号化・復号化記録装置の模式図である。

【図１６】本発明の第１実施形態の第２変形例に係る、

58

ＣＤ－Ｒ又はＣＤ－ＲＷのコピー防止方法のフローチャートである。

【図１７】本発明の第１実施形態の第３変形例に係る暗号化・復号化記録装置の模式図である。

【図１８】本発明の第１実施形態の変形例に係る、ＣＤ－Ｒ又はＣＤ－ＲＷのコピー防止方法のフローチャートである。

【図１９】本発明の第２実施形態に係る音響装置の模式図である。

【図２０】本発明の第２実施形態に係る他の音響装置の模式図である。

【図２１】本発明の第２実施形態の第１変形例に係る音響・映像・データ装置の模式図である。

【図２２】本発明の第２実施形態の第２変形例に係る音響・映像・データ装置の模式図である。

【図２３】本発明の第３実施形態に係る暗号化・復号化装置の模式図である。

【図２４】ＣＤ－Ｒ／ＲＷの非データ領域と、データ領域との配置を示す図である。

【図２５】書き込み途中におけるディスクのデータ構造を示す図である。

【図２６】書き込み終了後におけるディスクのデータ構造を示す図である。

【図２７】サブコーディングフレームのフォーマットを示す図である。

【図２８】フレームの詳細なフォーマットを示す図である。

【図２９】サブコーディング領域を詳細に示した図である。

【図３０】Ｑチャネルのモード１のフレーム構造を示す図である。

【図３１】Ｑチャネルのモード２のフレーム構造を示す図である。

【図３２】ドライブ装置がＭＣＮを記録する際のデータフォーマットを示す図である。

【図３３】ドライブ装置が読み込んだＭＣＮデータのフォーマットを示す図である。

【図３４】Ｑチャネルのモード３のフレーム構造を示す図である。

【図３５】ドライブ装置が読み込んだＩＳＲＣデータのフォーマットを示す図である。

【図３６】データ記録の第１の例を示す図である。

【図３７】データ記録の第２の例を示す図である。

【図３８】データ記録の第３の例を示す図である。

【図３９】（ａ）～（ｃ）は、それぞれ、３種類の暗号化キーを用いた暗号化キー生成方法の説明図である。

【図４０】ハッシュ関数のプログラム例を示す図である。

【符号の説明】

１，１′　メディア番号（メディア番号領域）

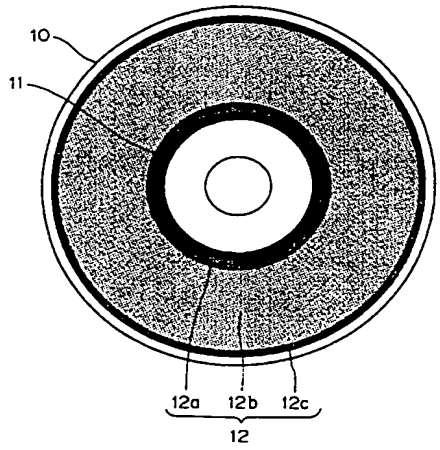
59

１０，１０′，６０　ディスク（メディア）
１１，６１　管理領域
１２，６２　ユーザ領域
１２ａ，６２ａ　リードイン領域
１２ｂ，５４ａ，６２ｂ　データ領域
１２ｃ，６２ｃ　リードアウト領域
１９　暗号化キー刷り込み装置
２０　パソコン
２０ａ，２３ａ，４２ｂ　暗号化メディア情報生成手段
２０ｂ，２３ｂ　暗号鍵生成手段
２０ｃ，４２ｆ　復号化手段
２０ｄ，４２ｅ　第２暗号鍵生成手段
２１ａ，３１ａ，４７ａ　ＣＤ－Ｒディスク（ＣＤ－Ｒメディア）
２１ｂ，３１ｂ，４７ｂ　ＣＤ－ＲＷディスク（ＣＤ－ＲＷメディア）
２２，４２，４６　ＣＤ－Ｒ／ＲＷドライブ
２２ａ，４２ａ　読出手段
２２ｂ，４２ｃ　暗号化メディア情報保存手段
２３　インターネットサーバ
２４　ＣＤドライブ

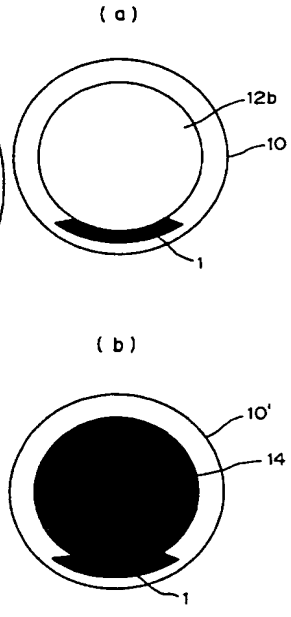
60

２６　データ送出装置
２７，２７ａ　音響装置
２８ａ，２８ｂ　スピーカー
２９　音響再生機器
３３　ＣＤ－Ｒ／ＲＷドライブ付きテレビ
３２　音響・映像・データ装置
３３ａ，３３ｂ，３３ｃ，４３，４３ａ，４３ｂ　ケーブル
３４　ＡＶ装置
３５　周辺記憶装置
３６，３６ａ　回線
４０，４０ａ，４０ｂ　暗号化・復号化記録装置
２２ｃ，４２ｄ　第２読出手段
４５　メディア番号設定手段
５３　ブロック
５３ａ　フレーム
５４　サブコーディング領域
５４ｂ　領域
５５　モード１のフレーム
５６　モード２のフレーム
５７　モード３のフレーム

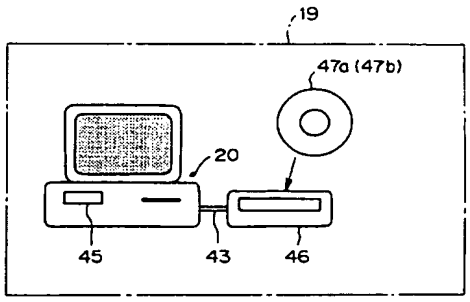
【図１】



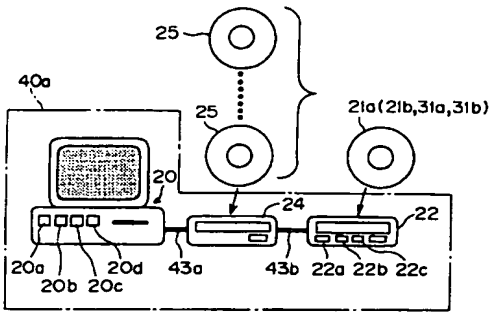
【図２】



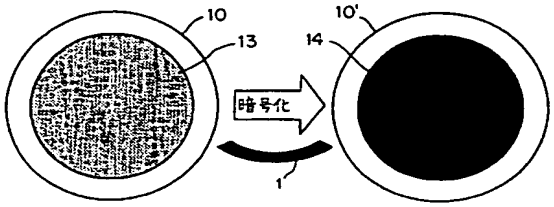
【図７】



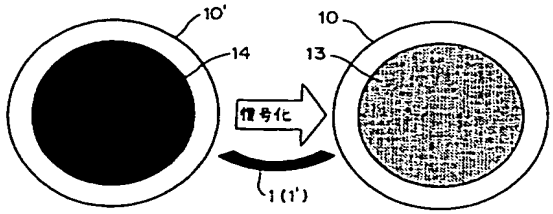
【図１５】



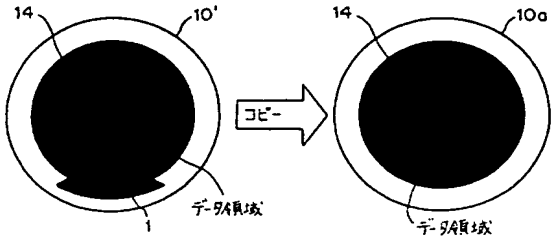
【図３】



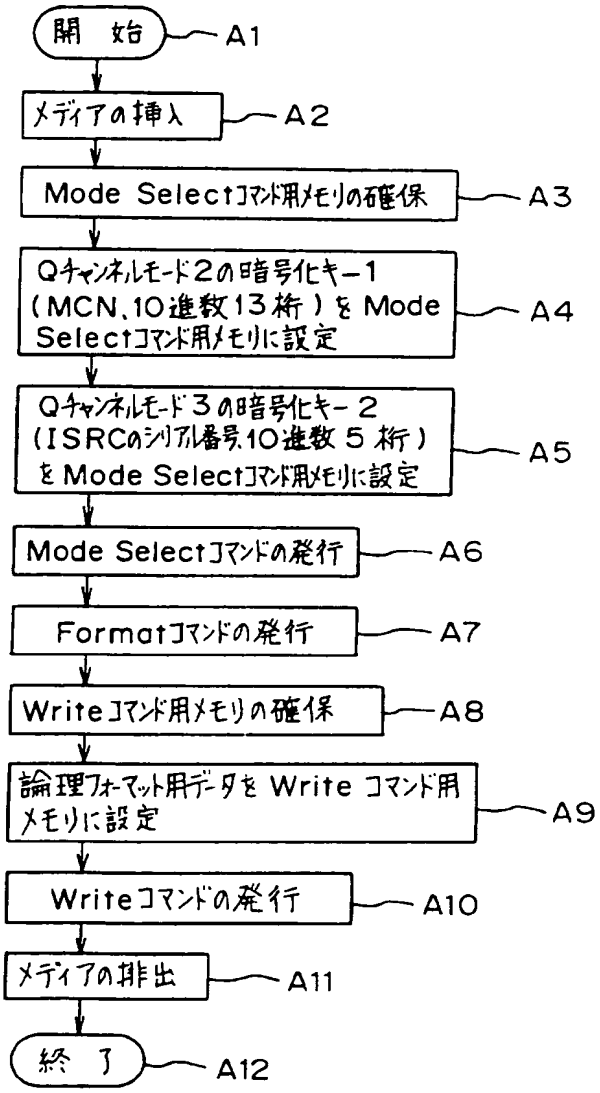
【図４】



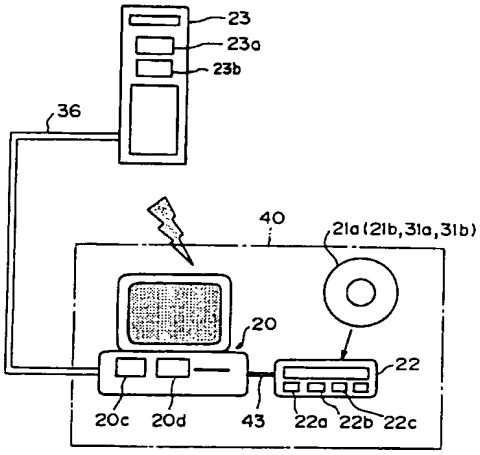
【図５】



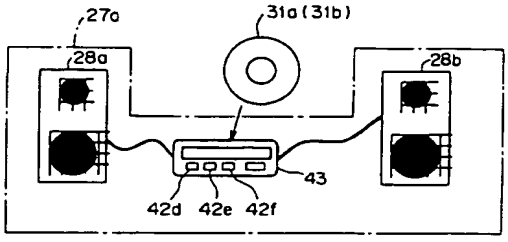
【図８】



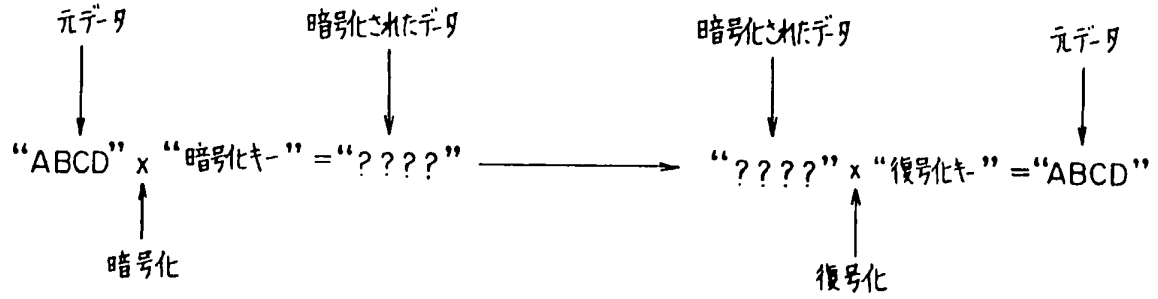
【図１３】



【図２０】



【図6】



【図39】

(a) Case 1: 暗号化キー-1, 暗号化キー-2, 暗号化キー-3の単純加算

暗号化キー = 暗号化キー-1 + 暗号化キー-2 + 暗号化キー-3
(ユニークID) (ID1) (ID2) (ID3)

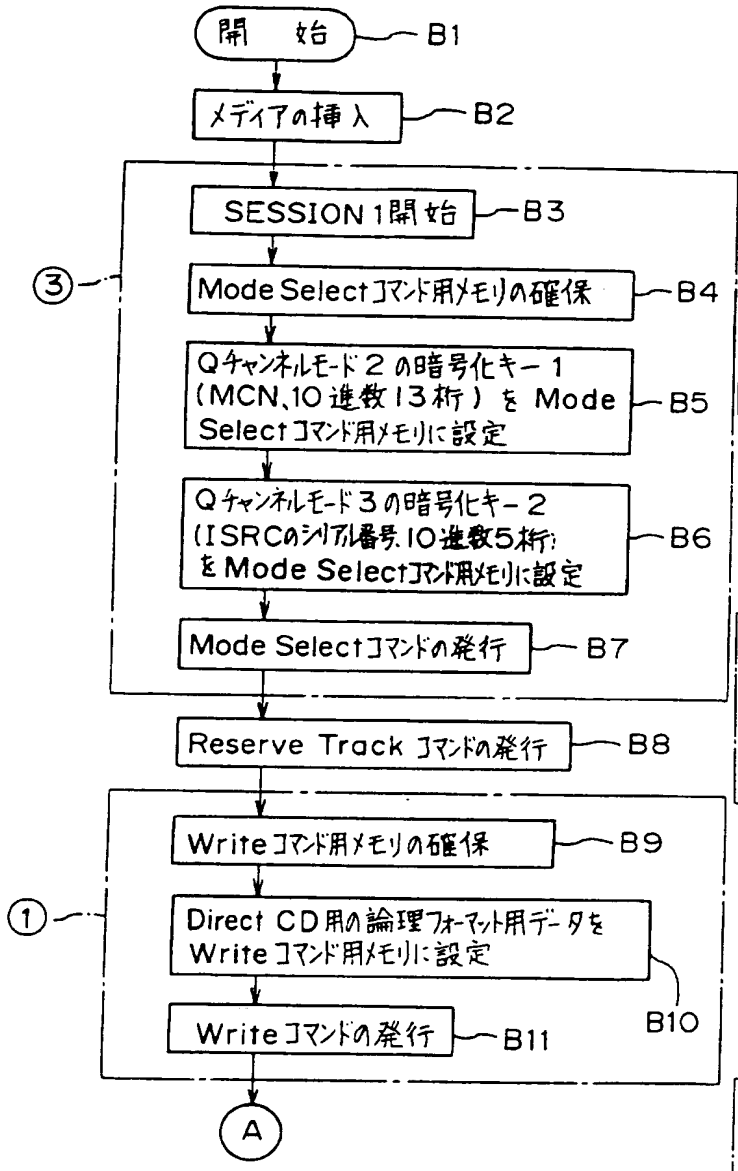
(b) Case 2: 暗号化キー-1, 暗号化キー-2, 暗号化キー-3を種として用いた乱数

暗号化キー = Rnd(暗号化キー-1) + Rnd(暗号化キー-2) + Rnd(暗号化キー-3)
(ユニークID) Rnd(ID1) Rnd(ID2) Rnd(ID3)
(Rnd( )は乱数関数)

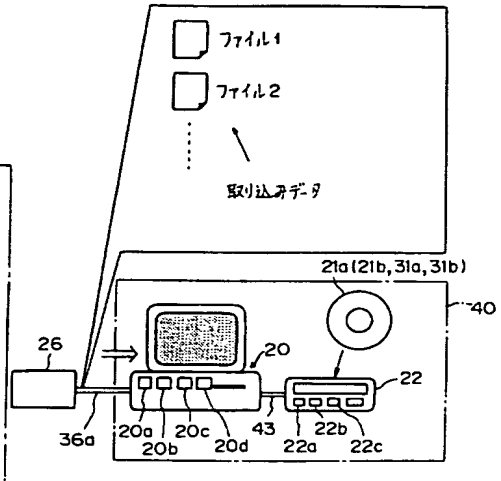
(c) Case 3: キーメッセージ及び暗号化キー-1, 暗号化キー-2, 暗号化キー-3を鍵として用いたハッシュ数

暗号化キー = Hash(キーメッセージ, 暗号化キー-1, 暗号化キー-2, 暗号化キー-3)
(ユニークID) hash(Key message, ID1, ID2, ID3)
(Hash( )はハッシュ関数)

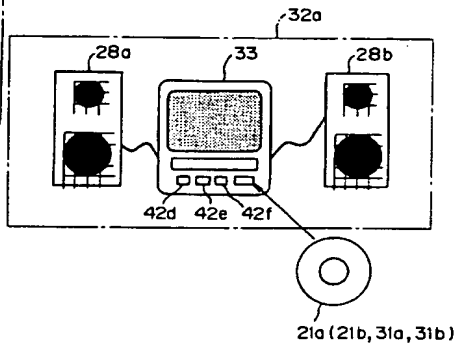
【図９】



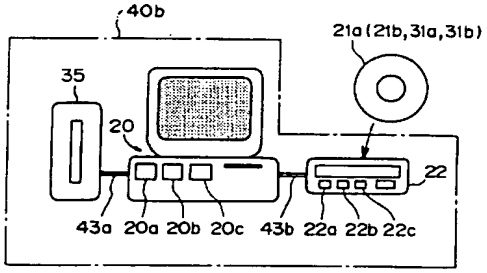
【図１７】



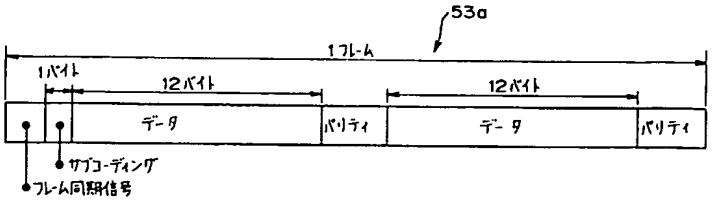
【図２２】



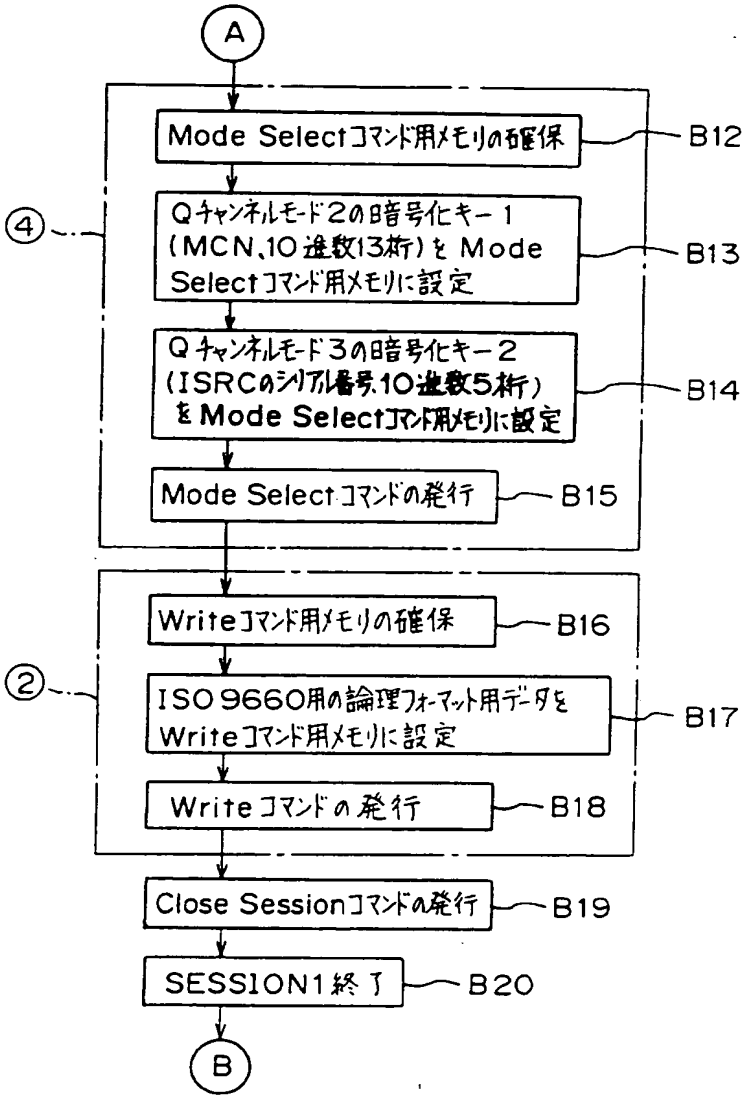
【図２３】



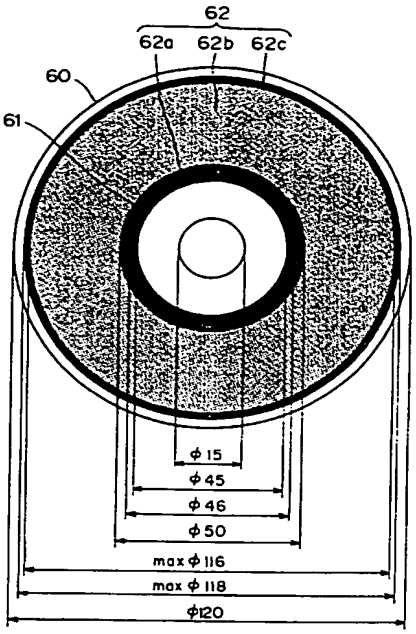
【図２８】



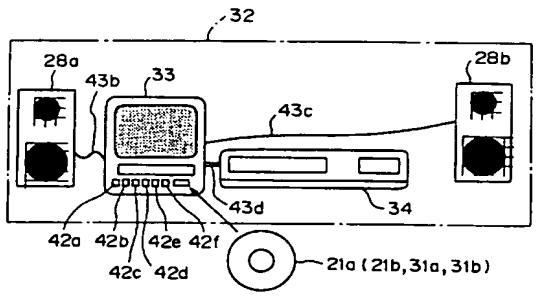
【図１０】



【図２４】



【図２１】

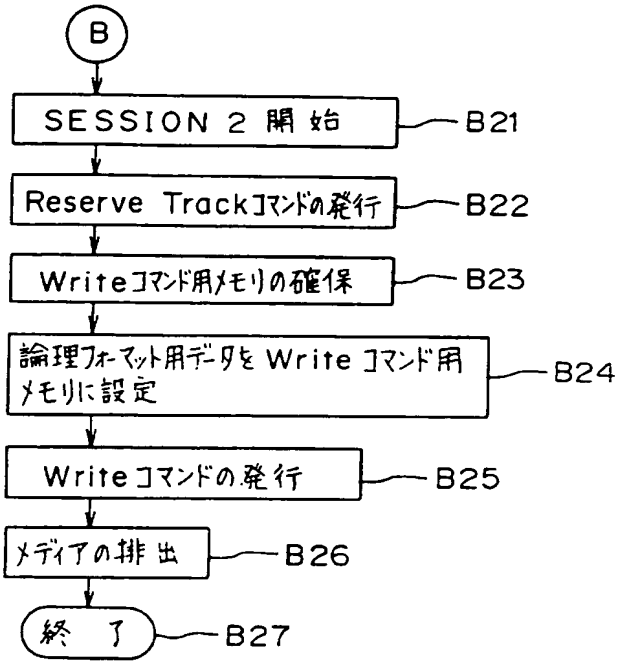


【図３２】

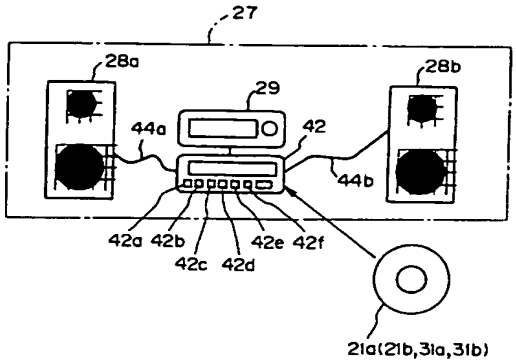
Media Catalogue Number data format

Byte \ Bit	7	6	5	4	3	2	1	0
0	Sub-Channel Data Format Code (02h)							
1	Reserved							
2	Reserved							
3	Reserved							
4 … 19	Media Catalogue Number (MCN)							

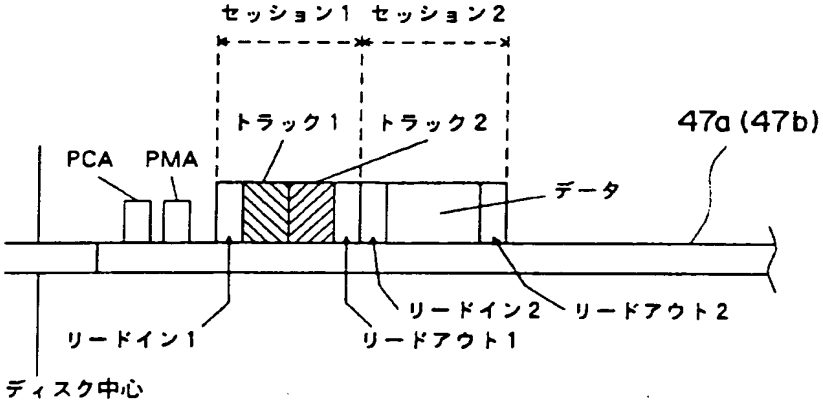
【図１１】



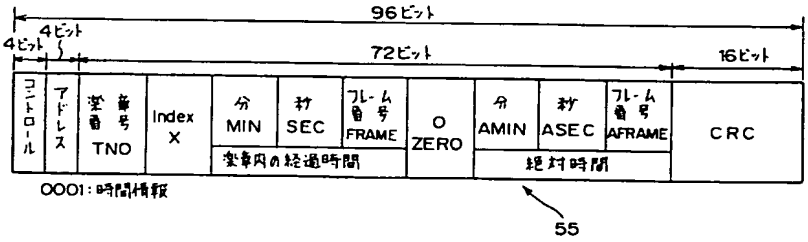
【図１９】



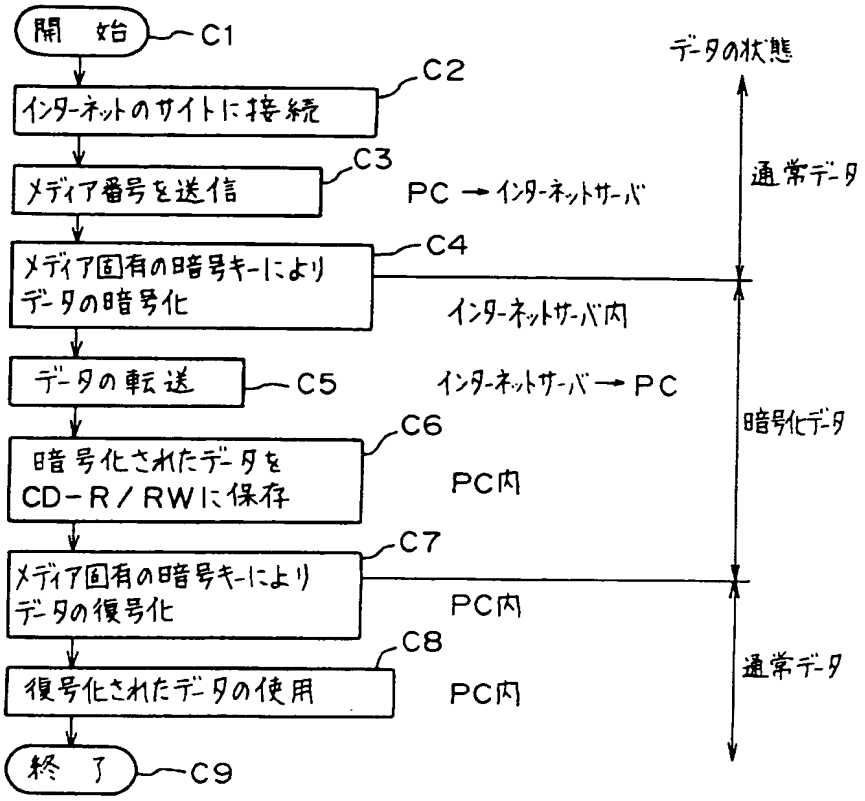
【図１２】



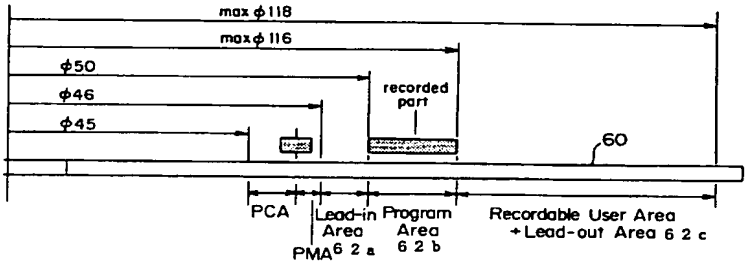
【図３０】



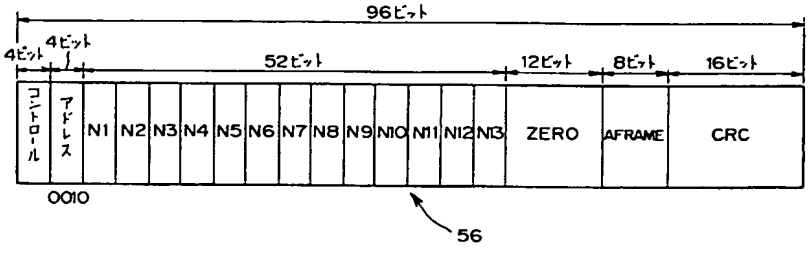
【図１４】


開　始
C1
インターネットのサイトに接続
C2
メディア番号を送信
C3
PC → インターネットサーバ
メディア固有の暗号キーにより
データの暗号化
C4
インターネットサーバ内
データの転送
C5
インターネットサーバ → PC
暗号化されたデータを
CD－R／RWに保存
C6
PC内
メディア固有の暗号キーにより
データの復号化
C7
PC内
復号化されたデータの使用
C8
PC内
終　了
C9
データの状態
通常データ
暗号化データ
通常データ

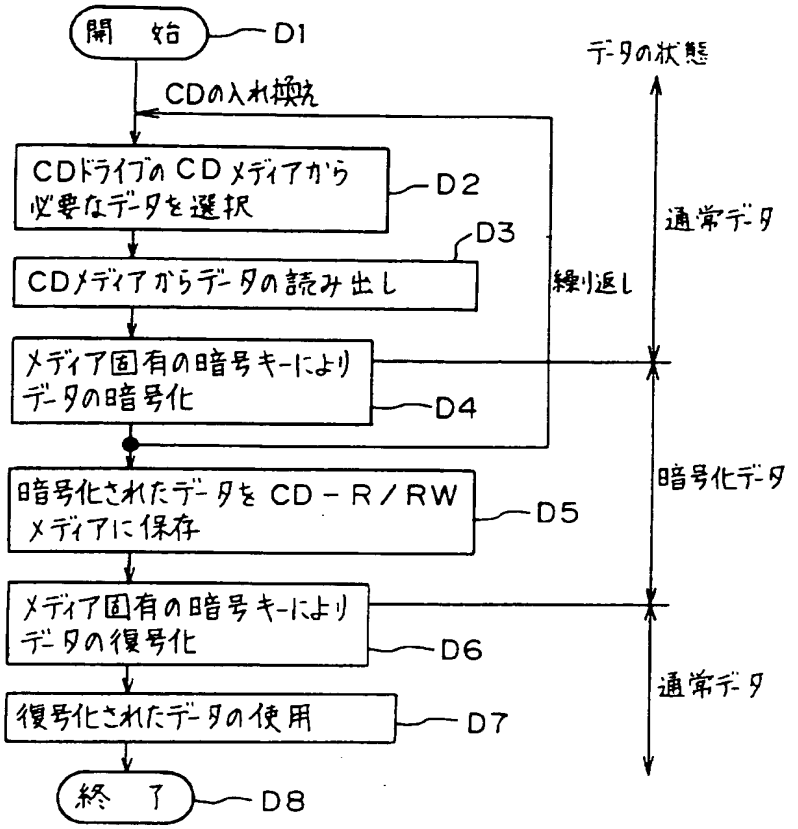
【図２５】


max φ118
max φ116
φ50
φ46
φ45
recorded part
60
PCA
Lead-in Area
PMA 6 2 a
Program Area 6 2 b
Recordable User Area + Lead-out Area 6 2 c

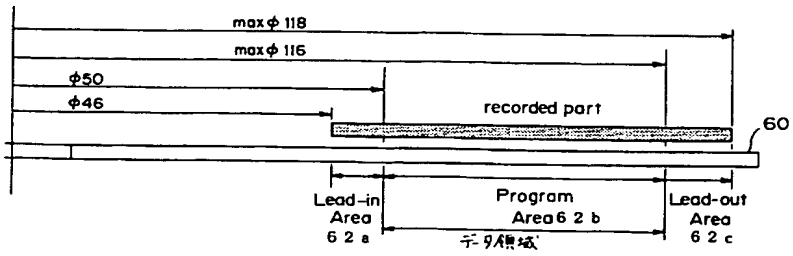
【図３１】


96ビット
4ビット
4ビット
52ビット
12ビット
8ビット
16ビット
コントロール
アドレス
N1 N2 N3 N4 N5 N6 N7 N8 N9 N10 N11 N12 N13
ZERO
AFRAME
CRC
0010
56

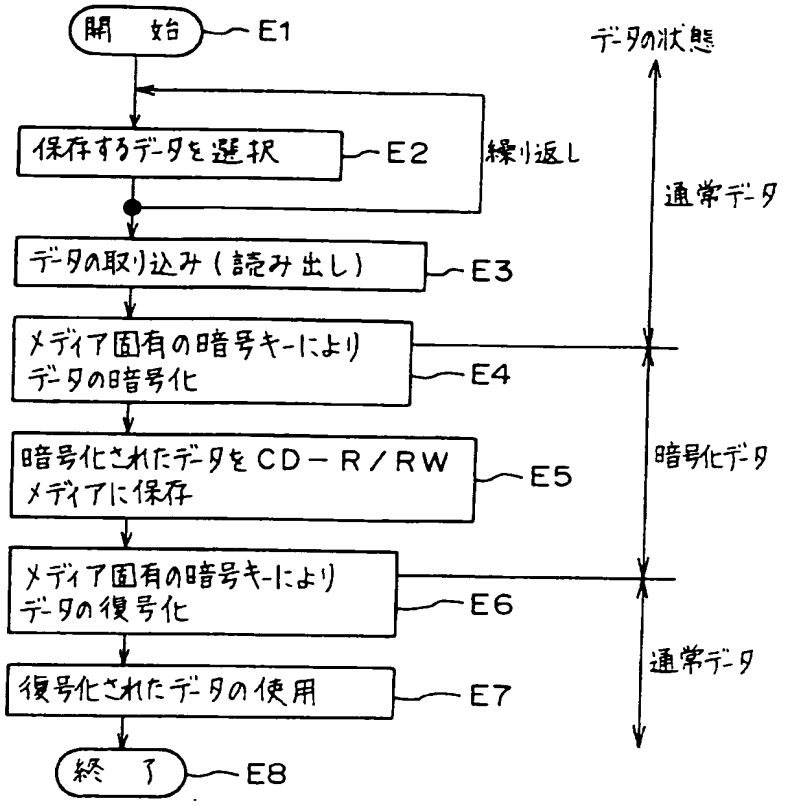
【図１６】


開　始
D1
CDの入れ換え
CDドライブのCDメディアから必要なデータを選択
D2
CDメディアからデータの読み出し
D3
メディア固有の暗号キーによりデータの暗号化
D4
暗号化されたデータをCD－R／RWメディアに保存
D5
メディア固有の暗号キーによりデータの復号化
D6
復号化されたデータの使用
D7
終　了
D8
データの状態
通常データ
繰り返し
暗号化データ
通常データ

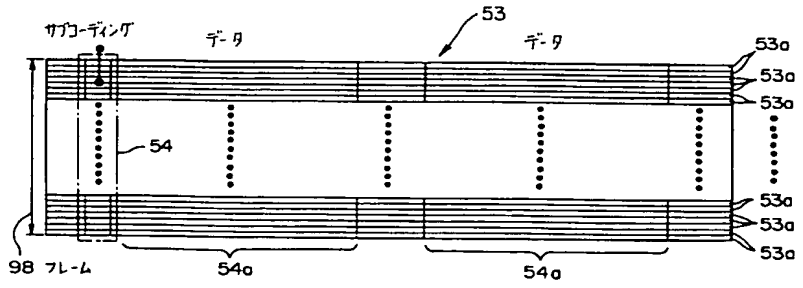
【図２６】


max φ 118
max φ 116
φ50
φ46
recorded part
60
Lead-in Area 62a
Program Area 62b
Lead-out Area 62c
データ領域

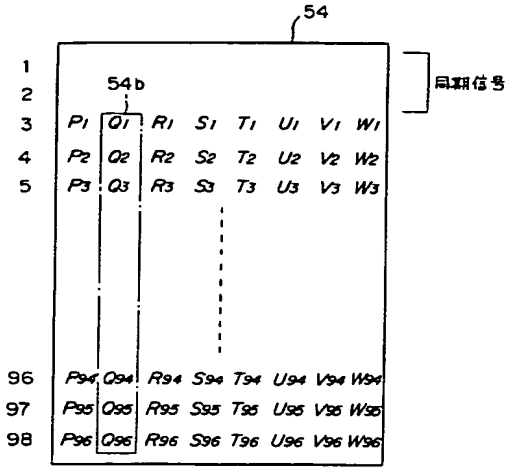
【図１８】


開　始
E1
保存するデータを選択
E2
繰り返し
データの取り込み（読み出し）
E3
メディア固有の暗号キーにより
データの暗号化
E4
暗号化されたデータをCD－R／RW
メディアに保存
E5
メディア固有の暗号キーにより
データの復号化
E6
復号化されたデータの使用
E7
終　了
E8
データの状態
通常データ
暗号化データ
通常データ

【図２７】


サブコーディング
データ
53
データ
53a
53a
53a
54
53a
53a
53a
98 フレーム
54a
54a

【図２９】



【図３５】

ISRC Format of Data Returned

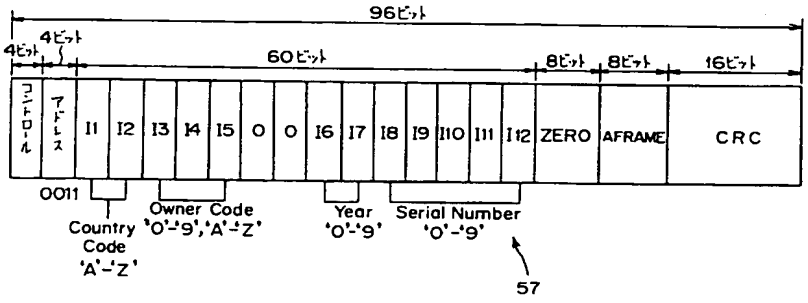
Byte	Char	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0		TCVAL	Reserved						
1	I1	I1 (Country Code)							
2	I2	I2							
3	I3	I3 (Owner Code)							
4	I4	I4							
5	I5	I5							
6	I6	I6 (Year of Recording)							
7	I7	I7							
8	I8	I8 (Serial Number)							
9	I9	I9							
10	I10	I10							
11	I11	I11							
12	I12	I12							
13		Zero							
14		AFRAME							
15		Reserved							

【図３３】

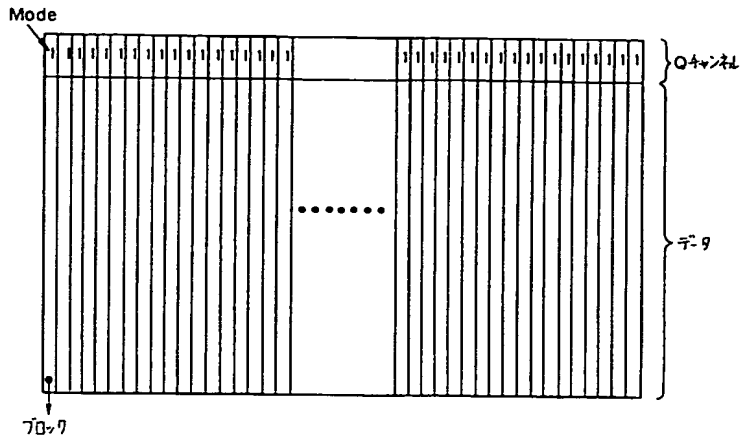
MCN Format of Data Returned

Byte	Char	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0		MCVAL	Reserved						
1	N1	N1 (Most significant)							
2	N2	N2							
3	N3	N3							
...	...	...							
12	N12	N12							
13	N13	N13 (Least significant)							
14		Zero							
15		AFRAME							

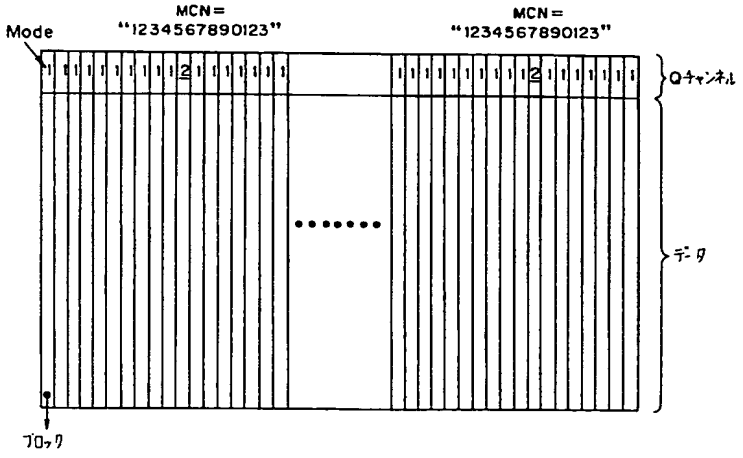
【図３４】



【図３６】



【図３７】

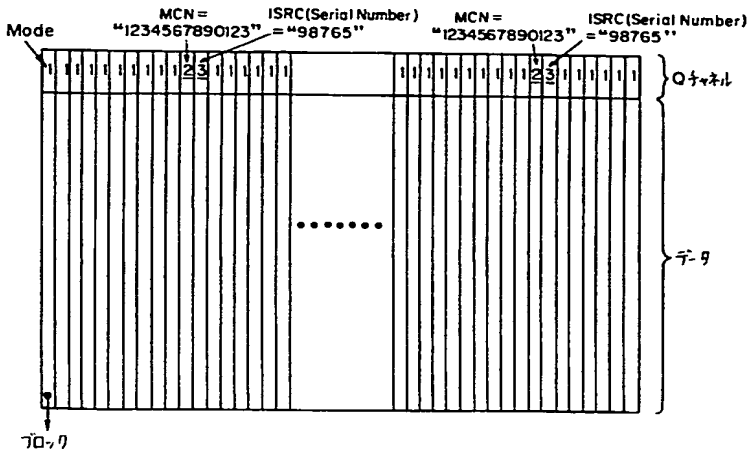


【図４０】

```
int func (char *str)
{
    int         val;
    int         len;
    if (str == NULL){
        return 0;
    }

    len = strlen(str);
    val = (*str-'a')+(*(str+len/2)-'a') * 26 + (*(str+(len-1))-'a') * 26 * 26;
    return val % SIZE;
}
```

【図３８】



フロントページの続き

(51) Int. Cl.[7]	識別記号	F I		テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｄ	

Ｆターム(参考)　5B017 AA03 BA07 CA09
5D044 AB01 AB05 AB07 BC04 CC06
DE02 DE50 DE55 DE57 DE58
DE83 EF05 FG18 GK12 GK17
HH13 HL04 HL08
5D110 AA16 AA17 AA27 AA29 DA08
DA10 DB03 DB18 DC05 DC15
5J104 AA01 AA13 AA16 EA02 EA04
EA26 FA07 NA02 NA12 NA17
NA32 PA14